Support Element (SE)

Version 2.16.0 - 17 May 2023

Contents

Support Element (SE)..... 1
Introduction..... 1
Introduction..... 1
User Interface..... 275
User Interface..... 275
Tasks..... 301
SE Tasks..... 301

Index..... 992

Support Element (SE)

The Support Element (SE) is located inside of the same frame that the system is located and is used to monitor and operate a system.

Learn how the SE applies many of its functions as described from the introductory material and explains how the tasks are used for the system.

Introduction

Introduction

You can expand this section for an overview of the Support Element (SE).

What's new in version 2.16.0

This guide reflects the licensed internal code for Support Element Console Application, Version 2.16.0. You can tell if your Support Element console has this version installed by looking at the title bar on the Support Element Console Workplace window or by pointing your mouse over **SE Version** in the top of the work pane window. New enhancements to the version code are described in this section.

There might be other changes to the licensed internal code that are not described in this guide. For additional information, refer to the PDF files available on Resource Link® at (http://www.ibm.com/servers/resourcelink) or the other documents shipped with your processor.

The following information summarizes the new and changed features for Version 2.16.0.

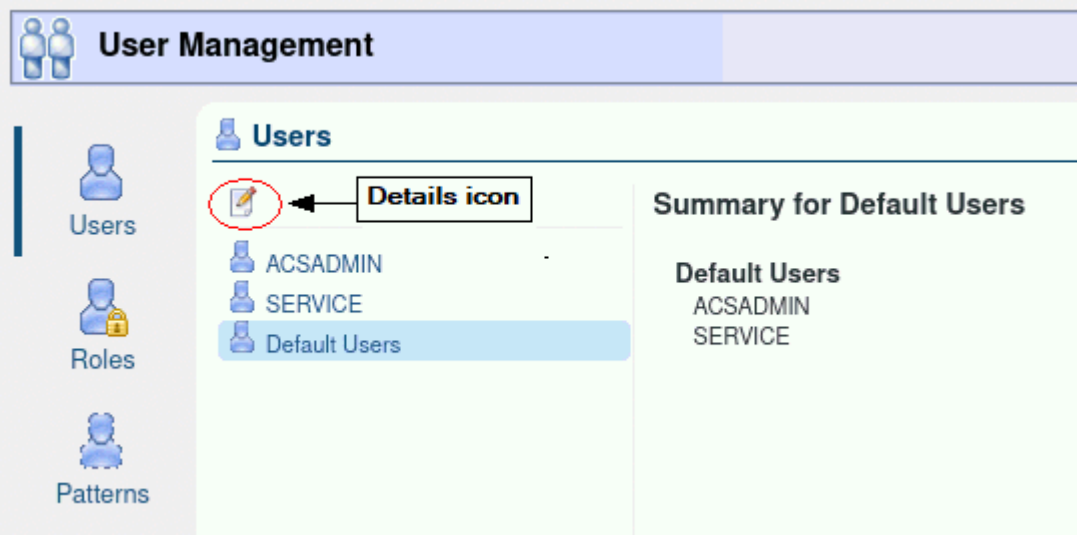
User Security: New requirement to change default passwords

Reduction of default user IDs for new HMC installs improves security without compromising control. SYSPROG, OPERATOR, and ADVANCED IDs are no longer included but are maintained on an upgrade or data replication from previous configurations.

All default users are required to change their passwords at the time of initial logon. The **User Management** task adds additional function to accomplish this function. The only users that can access the additional function are SERVICE or a user that is assigned a role with Manage Users task permission.

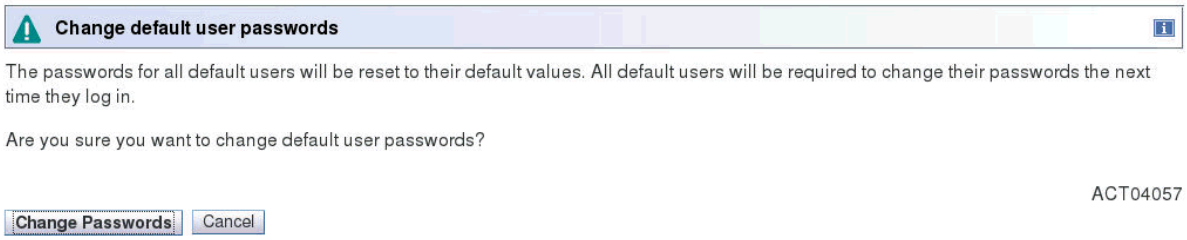
To force the default user IDs to change their passwords on their next login:

1. Log on with SERVICE or a user that is assigned a role with permission to manage users.
2. Go to the **User Management** task.
3. If you are logged in as a user that is assigned a role with Manage Users task permission, select **Default Users**, which display the list of default users the password change affects.

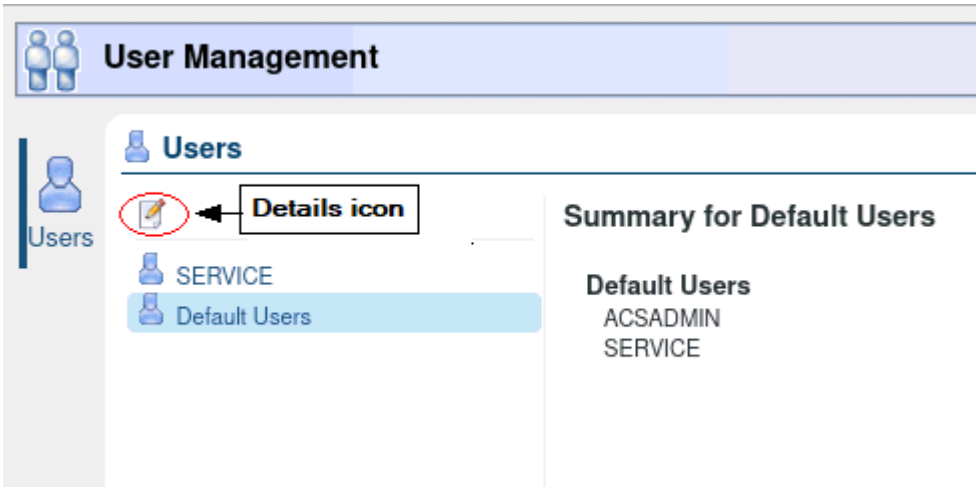


a. Click the **Details** icon. The Change default user passwords window is displayed.

b. Click **Change Passwords** to reset all system defined user passwords back to their defaults and force those user IDs to change their password the next time they logon.

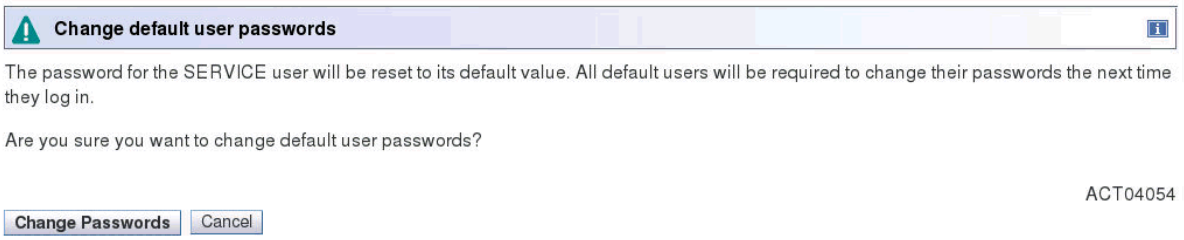


4. If you are logged in as SERVICE, select **Default Users**, displays the list of default users the action affects.

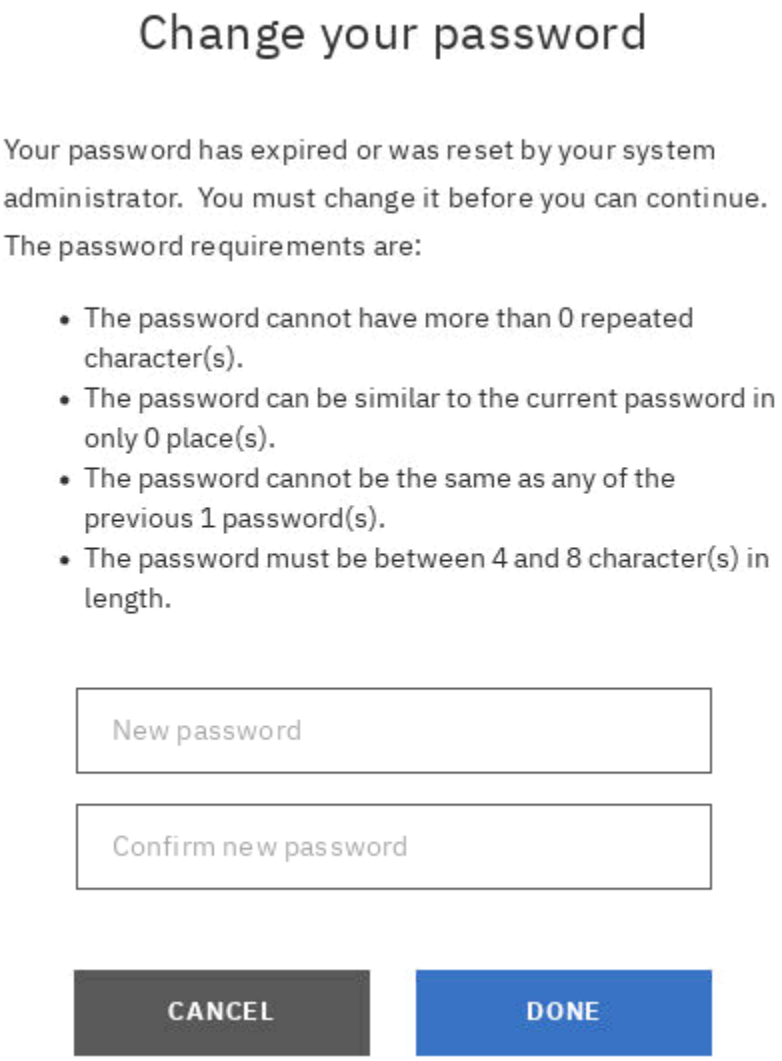


a. Click the **Details** icon. The Change default user passwords window is displayed.

b. Click **Change Passwords** to reset only the SERVICE user's password back to its default and force all the other system defined default users to change their passwords the next time they logon.



As a result of the previous change passwords function, the following prompt is displayed after the default user ID initially logs on.



Elevate user authority using LDAP

Easily elevate or reduce a user's HMC task and resource authorizations. Elevated authority can be granted by an administrator using LDAP server group definitions. See the related videos in our HMC video library (http://ibm.biz/IBM-Z-HMC).

The enhancement of the User Patterns in the **User Management Task** is enhanced to allow the access administrator to specify the group-to-template mappings and the LDAP server is used for the group membership lookups. For ordered list-to-template mappings:

- Each entry maps an LDAP group name to an HMC User template name
- The intended use is for higher authority groups before lower authority groups.

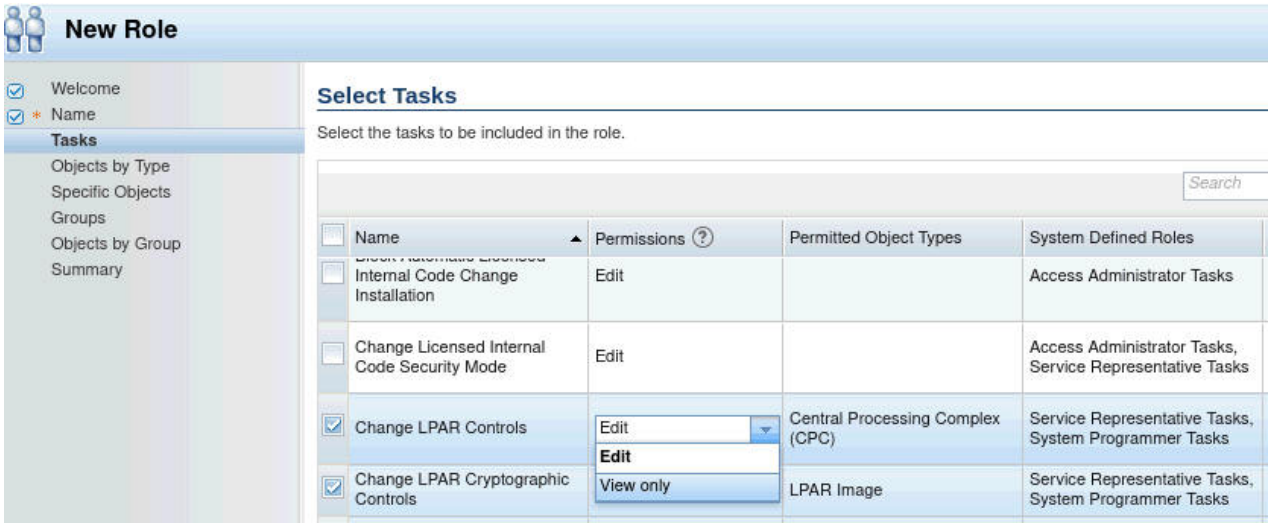
The Name of LDAP Server Definition for group lookups:

- Identifies the LDAP server that hosts the group entries
- Specifies how to find group entries and their member list.

Read-only access for Change LPAR Controls task

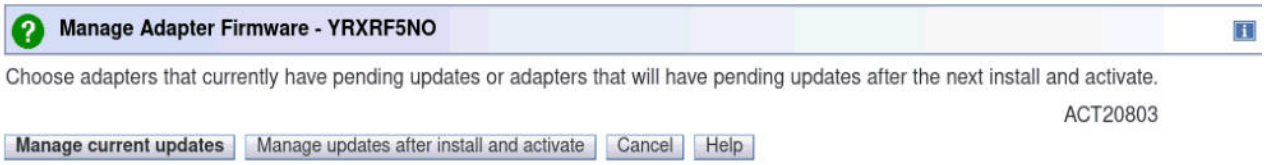
Securely view partition logical processor assignments with view-only support for **Change LPAR Controls** and **Change LPAR Group Controls** tasks.

Additional support for HMC view-only **Change LPAR Controls** and **Change LPAR Group Controls** tasks. The new view-only task selection for **User Management** task role is the single task name permissions assignment for tasks.



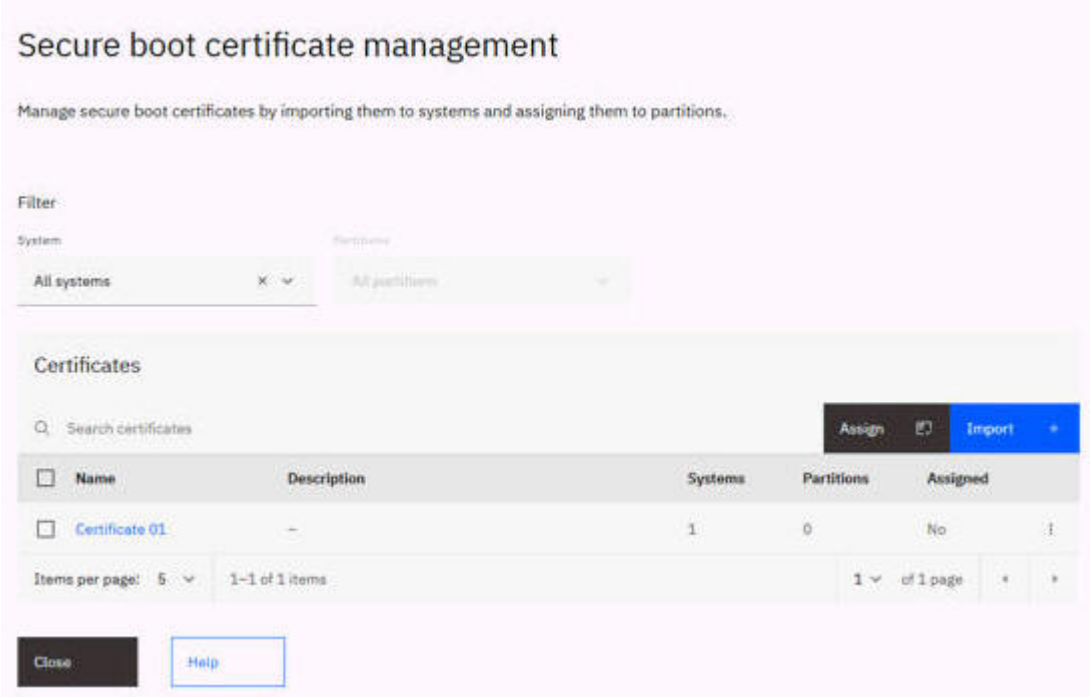
Manage Adapter Firmware task

The new **Manage Adapter Firmware** task allows the user to select one or more cryptos which are pending a firmware update. Provides a solution to continue through pending channels one at a time and toggle them off and on again to provide a simpler solution which can be concurrent to operating system activities if the system is configured with the appropriate redundancy. You can choose adapters current updates pending or adapters updates after the next install and activate. This task was previously the **Query Channel/Crypto Configure Off/On Pending** task.



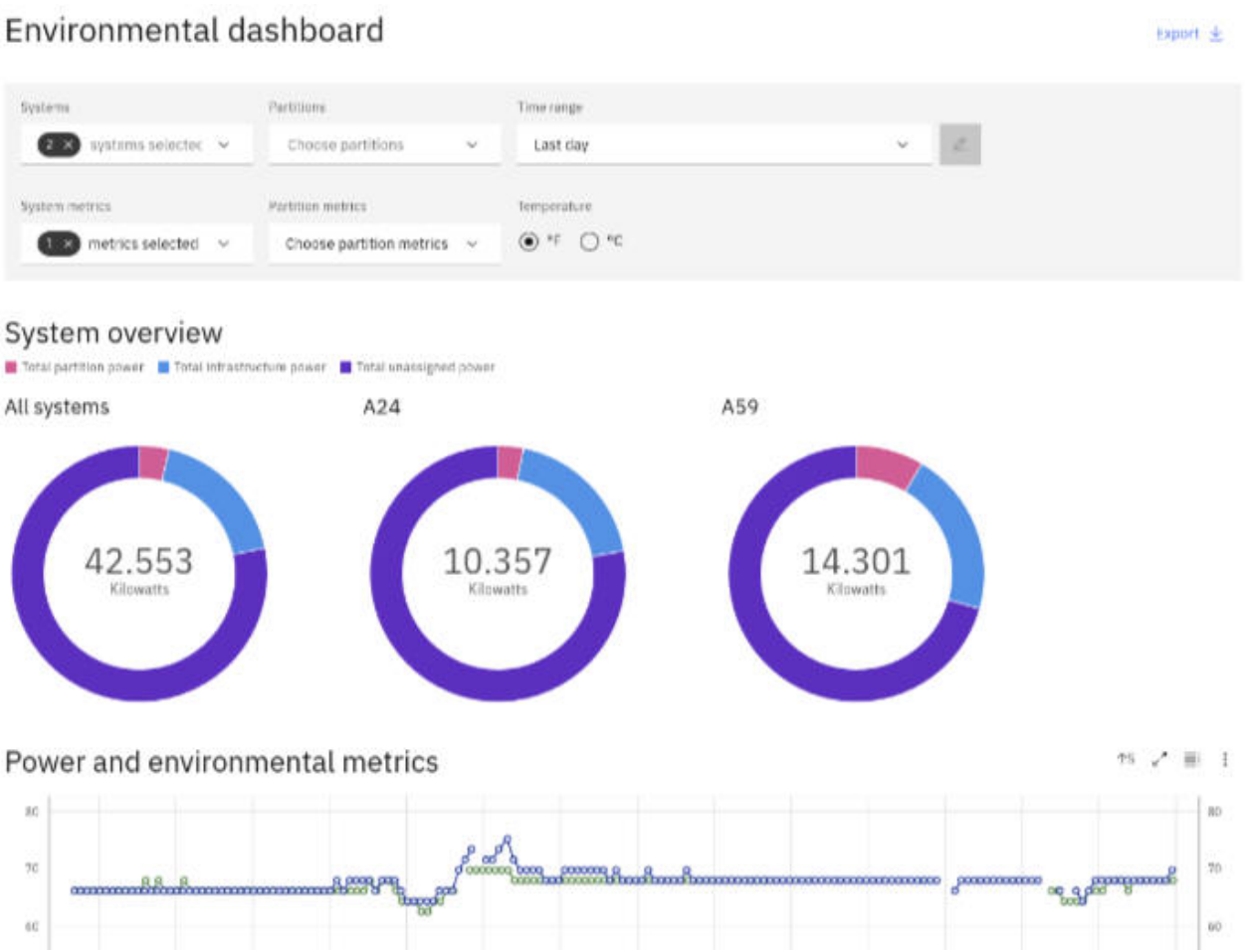
Secure boot certificate management task

The new **Secure boot certificate management** task allows the user to manage the secure boot certificate(s) used on your system. This task allows you to import certificates to your system, assign those certificates to partitions, image activation profiles, and PRSM2 partitions, or unassigned certificates for the system and associate partition.



Environmental dashboard task

The new **Environmental dashboard** task allows the user to integrate system and partition level power consumption metrics data, select time ranges for metrics view, display selected system and partition metrics in a line chart or tabular view, and export the metric data. This task replaces the **Environmental Efficiency Statistics** task.



Miscellaneous enhancements

The following miscellaneous changes are part of Version 2.16.0:

- The **Save/Restore Customizable Console Data** task added a table tool bar to the Customizable Data Types table to give you the ability to select all data types at once.
- The **Customize Console Services** task includes new services:
  - **Minimum TLS version** - you can specify the minimum TLS version that the console will negotiate.
  - **Transmit system availability data** - you can specify to send system availability data to the support system for analysis.
- The **Remote Service** task adds a new option, **Authorize service personnel to remotely request transmission of service data**. You can set the console to allow a service representative to remotely schedule firmware updates and then monitor the updates remotely.
- The **View PMV Records** task has been removed.
- The **Customize Scheduled Operations** task has removed the **Transmit system availability data** operation. This operation has been added to the **Customize Console Services** task as a new service.
- Starting with machine type 3931, the OSA-Express 1000 Base-T adapters for System Management (OSM) are no longer required to enable DPM mode on the system. The Support Element tasks **Enable Dynamic Partition Manager** and **System Details** no longer have controls for selecting the OSM adapters.
- The **Advanced Facilities** task added support to the view port parameters for the optical power measurement for both long distance and short distance coupling. A new Force port log option is added to the The Force Log window for long distance coupling card.

- The **Monitors Dashboard** task added new **Total Partition Power Consumption, Total Infrastructure Power Consumption** and **Total Unassigned Power Consumption** metrics to the Power Consumption table. The Logical Partition table added new **Power Consumption** metrics.
- The reset and image load pages of **Customize/Delete Activation Profiles** task and the **Load** task have been enhanced to allow a list-directed load or load dump from an ECKD device with secure boot selection. The load type filed is now broken into Device type, IPL type, and Load type. The **View Activation Profiles** task, **System Details** task, and **Image Details** task are enhanced to view the new load enhancement updates.

Introduction to the Support Element

A *Support Element* is a dedicated workstation that is used for monitoring and operating a system. If you have experience using other systems, you may have used a processor console, support processor, or a similarly named workstation to monitor and operate them.

This system is an *integrated Support Element*, that is, the Support Element is located inside the same frame that the system is located. An alternate Support Element is also provided to give you the option to switch from your primary Support Element to your alternate Support Element if hardware problems occur.

The IBM Z® and IBM LinuxONE (LinuxONE) systems operate only in logically partitioned mode.

A *Hardware Management Console* is required for monitoring and operating systems with integrated Support Elements.

The information that is provided here is for anyone who is responsible for monitoring and operating the IBM Z and LinuxONE systems.

It provides information and instructions for users who use a Support Element while logged on with a user ID assigned the following user roles:

Access Administrator Tasks
Advanced Operator Tasks
Operator Tasks
Service Representative Tasks
System Programmer Tasks

Notes:

- Beginning with Hardware Management Console Version 2.15.0, support is provided for n-2 system levels only. IBM z14® (HMC Version 2.14.1) is the last system to support four generations of systems (n through n-4).
- There are representations of the Hardware Management Console and Support Element windows displayed throughout this information. They may or may not represent the exact windows that are displayed for your user ID or version.
- Many of the same tasks and controls that are available in the user modes that are listed above are available also in the service representative user mode.

Support Element users should be familiar with using:

- CD-ROM
- Communication devices
- Direct access storage devices (DASD)
- DVD-RAM
- Graphical user interfaces
- Printers
- USB flash memory drive (formerly referred to as the memory key)
- Workstations

Note: If you are using a USB flash memory drive, plug it into the console and then wait for the console to beep three times. This indicates that the device is ready and can be accessed. If it does not beep three times, unplug the device and try again.

For information and instructions for operating devices other than the Support Element, refer to the documentation provided with the devices.

The Support Element Console Application

The Support Element Console Application version 2.16.0 is a licensed application that provides the tasks you will use to monitor and operate your system. The application is shipped with each Support Element.

The version number of the Support Element Console Application is displayed in the title bar of the Support Element Logon window and also the Support Element Workplace window.

The Support Element Console Application starts automatically whenever the Support Element is turned on or rebooted. Starting the application begins the process of initializing it. A window displays the company logo and copyright information. When the process completes, the logon window is displayed.

The Welcome window includes links for logging on to the Support Element console and to the online help. It also includes status indicators and message icons. The status indicator reflects the current overall status of the system and images. The message indicators alert you to any hardware or operating system messages. If any of these icons do not display a green check mark, you are alerted that a message was logged that may require your attention. See Figure 1 on page 8 for an example of the Welcome window.

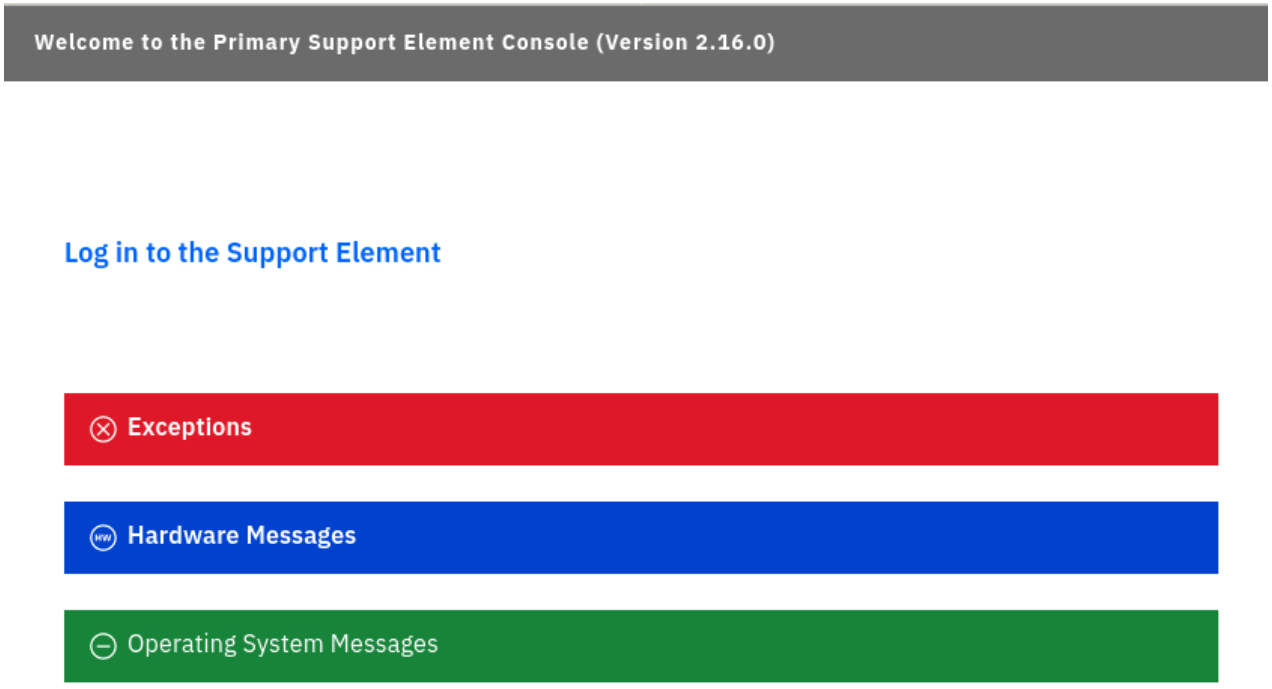


Figure 1. Support Element console welcome window

To log on to the Support Element console, click **Login to the Support Element** from the Welcome window. The Logon window is displayed.

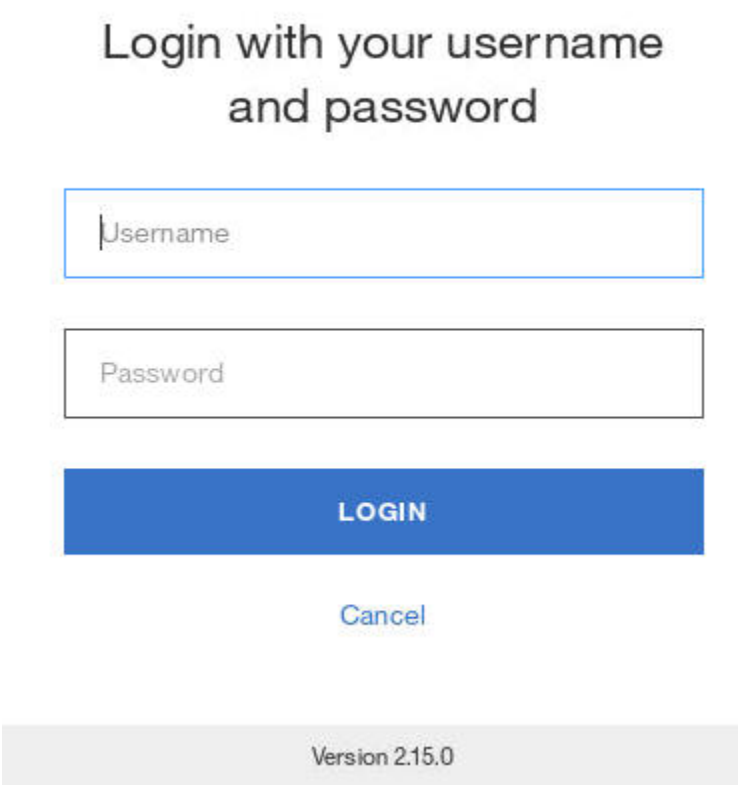


Figure 2. Support Element console logon window

Default user IDs and passwords are established as part of a base Support Element Console. The Access Administrator **should assign new user IDs and passwords for each user and change the default user IDs as soon as the Support Element Console is installed** by using the **User Management** task. The predefined default user roles, user IDs, and passwords are:

```
Access Administrator    ACSADMIN      PASSWORD
Service Representative  SERVICE       SERVMODE
```

Note: Letter case (uppercase, lowercase, mixed) is not significant for the default user IDs or passwords.

Attention: The use of default passwords are no longer allowed. The first time a default user ID logs on to the console, the default password must be changed. A prompt is displayed requiring the password change. This is initiated in the **User Management** task by SERVICE or a user that is assigned a role with Manage Users task permission.

The Support Element workplace is the window from where you start tasks for monitoring and operating the system. Your *user role* determines which tasks and controls you can use on the Support Element workplace. Not all tasks are available for each user role. Refer to the description of the specific task you want to access to see what user role(s) it is available in. Letter case (uppercase, lowercase, mixed) is not significant for the default user IDs or passwords.

If at any time you do not know what user ID is currently logged on to the Support Element console, click on the user ID located on the task bar.

Establishing a Support Element console session from a Hardware Management Console

A Hardware Management Console must be used for monitoring and operating systems with integrated Support Elements.

Ordinarily, you should use the Hardware Management Console to monitor status and perform tasks for the systems defined to it. Only the Hardware Management Console can be used for monitoring and operating multiple systems; using it is more efficient than using each system's Support Element console individually.

Using a system's Support Element console is necessary only for getting information or using tasks that are *not* available from the Hardware Management Console. If using a system's Support Element console is necessary, use the Hardware Management Console's Single Object Operations task to establish a session with the Support Element console. The Single Object Operations Task Confirmation window displays. Follow the instructions on the Confirmation window to complete this task.

Logging on to the Support Element with a Hardware Management Console user name

When you log on to the Support Element with a Hardware Management Console user name, the following scenarios are considered.

- When the Support Element does not have a user name that matches the Hardware Management Console user name, the Support Element attempts to match to the Hardware Management Console user name based on the user name and password that is provided on the Support Element log on prompt. The Support Element user name is created dynamically with permissions based on the Hardware Management Console user name.
  - If a single Hardware Management Console user name matches both the user name and password on the Support Element, then this user name is logged on to the Support Element.
  - If multiple Hardware Management Console user names match both the user name and password on the Support Element, then the matching user names are compared based on properties such as permissions or settings.
    - If all matching user names have the same properties, then the user name from the Hardware Management Console that most recently targeted the Support Element is used.
    - If at least one user name has different properties, then a user name cannot be chosen and that user name cannot log on to the Support Element.
- As you attempt to log on to the Support Element with a Hardware Management Console user name and password, the appropriate audit logs are displayed.

Logging off the Support Element Console

Once you have completed using the Support Element, you may end the current user session and either log off or disconnect from the console using the **Logoff or Disconnect** task.

Disconnecting preserves your session and allows your tasks to continue running without user accessing to the console. Disconnect sessions exist while the Support Element console application is running. If the Support Element console is restarted or the console is shut down, all session information is lost.

If you disconnect, you can reconnect at a later time. When you login again, a Choose a Disconnected Session window is displayed. You can select the disconnected session to continue working or you can begin a new session. (The number of windows displayed depends on the state of the session when it was disconnected. One of the windows is the main user interface; additional windows are for each task that was running when the session was disconnected.)

Logging off of the Support Element console terminates all running Support Element application tasks and ends the session. The log off operation should only be used when you no longer need access to the Support Element console. Logging off of the console does not affect the status of the CPC or images.

The Support Element workplace window closes and the Hardware Management Console workplace window is displayed.

To log off the Support Element console:

1. Open the **Logoff or Disconnect** task. The Choose to Logoff or Disconnect window is displayed.
2. Select **Log off**.
3. Click **OK** to end your session on the Support Element console.

To disconnect from the Support Element console:

1. Open the **Logoff or Disconnect** task. The Choose to Logoff or Disconnect window is displayed.
2. Select **Disconnect**.
3. Click **OK** to disconnect from your session on the Support Element console with the intent of returning at a later time.

Supported character sets

The console only supports Single-Byte Character Sets (SBCS) for data entry.

Using a remote Support Element

Table 1 on page 11 and Table 2 on page 11 shows the ports a remote Support Element uses for communications.

Table 1. Support Element inbound traffic from customer networks

TCP/IP Source Port	Usage
ICMP Type 8	Establish communications with Hardware Management Consoles (HMCs) managing the server.
tcp/udp 58787	Automatic discovery of system resources by HMCs.
tcp 55555	SSL encrypted communications from Hardware Management Consoles.
tcp 9920	SSL encrypted communications from Hardware Management Consoles.
tcp 443	Remote user access to the Support Element. Inbound traffic for this port is only allowed by the internal firewall if the **Single Object Operations** task is performed to the Support Element from the HMC.
udp 161 tcp 161 tcp 3161	SNMP automation. Inbound traffic for these ports is only allowed by the internal firewall when SNMP automation is enabled by using the **Customize API Settings** task.
udp 520	Interactions with routers and only used on the Support Element if **'routed'** is enabled in the **Customize Network Settings** task.
tcp 22	Remote access by Product Engineering and only allowed by the internal firewall if remote product engineering access is configured using the **Customize Product Engineering Access** task.

Table 2. Support Element outbound traffic to customer networks

TCP/IP Source Port	Usage
ICMP Type 8	Establish communications with Hardware Management Consoles (HMCs) managing the Support Element.
tcp 58787 - 58788 udp 58788	Automatic discovery of system resources by HMCs.
tcp 55555	SSL encrypted communications to Hardware Management Consoles.
tcp 9920	SSL encrypted communications to Hardware Management Consoles.
tcp 21	Load system software or utility programs.
tcp 22	Retrieve the SSH public key of hosts, using the **Manage SSH Keys** task, for securing SFTP connections to FTP servers. Also, used for the SFTP connections.

Table 2. Support Element outbound traffic to customer networks (continued)	
TCP/IP Source Port	**Usage**
udp 520	Interactions with routers and only used on the Support Element if **'routed'** is enabled in the **Customize Network Settings** task.
udp 123	Sets the time of the Support Element from the HMC.

Context sensitive help

Context sensitive help allows you to view abbreviated help information for input fields or selectable fields that appear on the task window. To enable this function:

1. Click on the blue **i** that is displayed in the upper right corner of the task window (see Figure 3 on page 12). Every time a new task window opens you need to click **i** to enable context sensitive help.

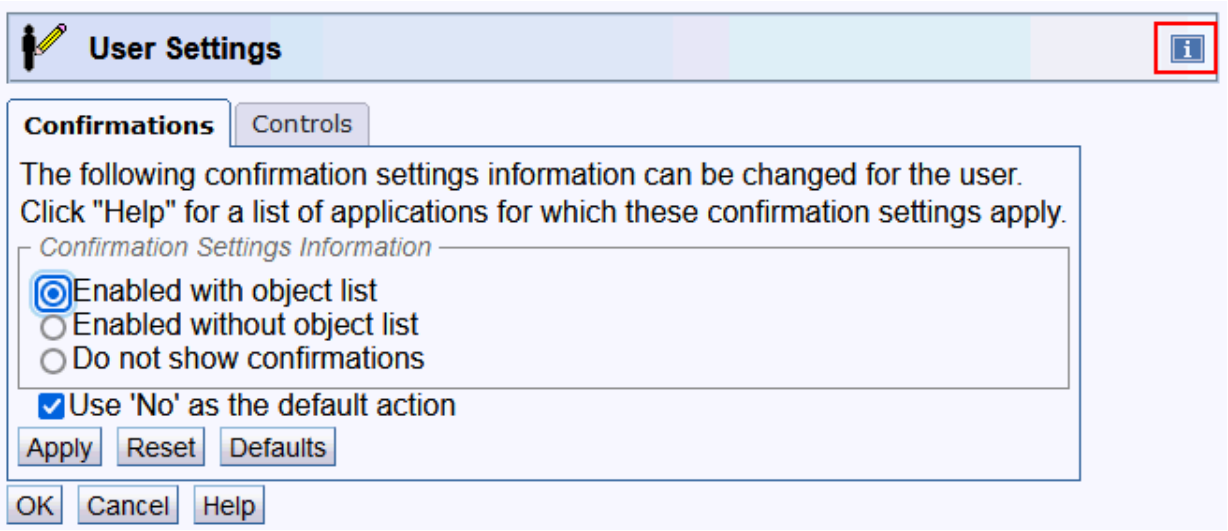


Figure 3. Context sensitive help not enabled

2. Once context sensitive help is enabled the **i** in the upper right corner of the task window changes to an orange **?**. As you place your cursor over the input fields or selectable fields the abbreviated help text is displayed in a small box within the task window (see Figure 4 on page 12). Using the Tab key also allows you to view the help for each field. As you tab to each field, context sensitive help is displayed.

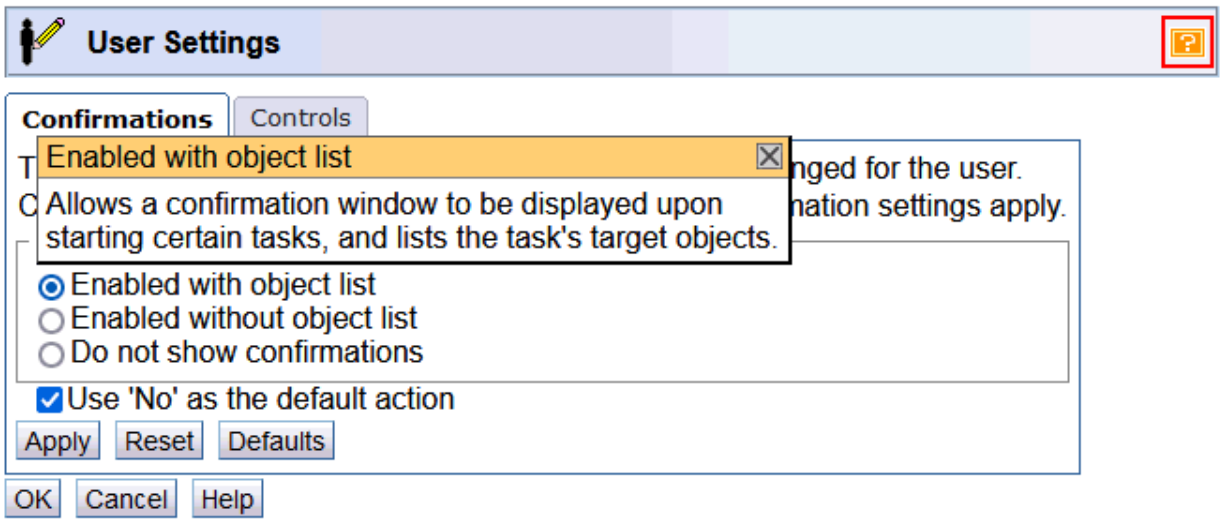


Figure 4. Context sensitive help enabled

- You have the capability to move the help box if it hides some of the information on the task window. As you move your cursor into the help box area the cursor will change from an arrow to a yellow cross arrow. Holding the left mouse button down within the box allows you to drag the box to a more convenient area in the task window.
- You can close the help box by clicking on the **X** in the upper right corner. This will not disable the context sensitive help for the task window, it just removes the help box for the item you were getting help on.
- Scroll bars can be used on the bottom and side of the task window for expanding the task window and allowing more area to view the help box.
- You can continue to perform task options while the context sensitive help is enabled.

3. When you are ready to disable context sensitive help for the task window, click on the **?**.

Disruptive tasks

Some of the Support Element tasks can be considered *disruptive*. Some of these tasks include:

- **Daily Tasks:** Activate, Deactivate, Reset Normal
- **Recovery Tasks:** Load, Load from Removable Media or Server, PSW Restart, Reset Clear, Reset Normal, Start All, Stop All
- **Change Management Tasks:** Change Internal Code, Engineering Changes (ECs), Product Engineering Directed Changes, Single Step Internal Code Changes, Special Code Load
- **Operational Customization Tasks:** Configure Channel Path On/Off

Note: Launching the **Stop** task can be considered disruptive under the following circumstances:

- Targeting a system or partitions on which IBM® Dynamic Partition Manager (DPM) is enabled.
- Confirming changes from the **Adapter Details** window.

Performing a task on a CPC or CPC image might disrupt its operation. The Disruptive Task Confirmation window that is shown in Figure 5 on page 13 is an example of a disruptive task about to be performed on an object. In this particular case the user profile option to require password verification for disruptive tasks is enabled.

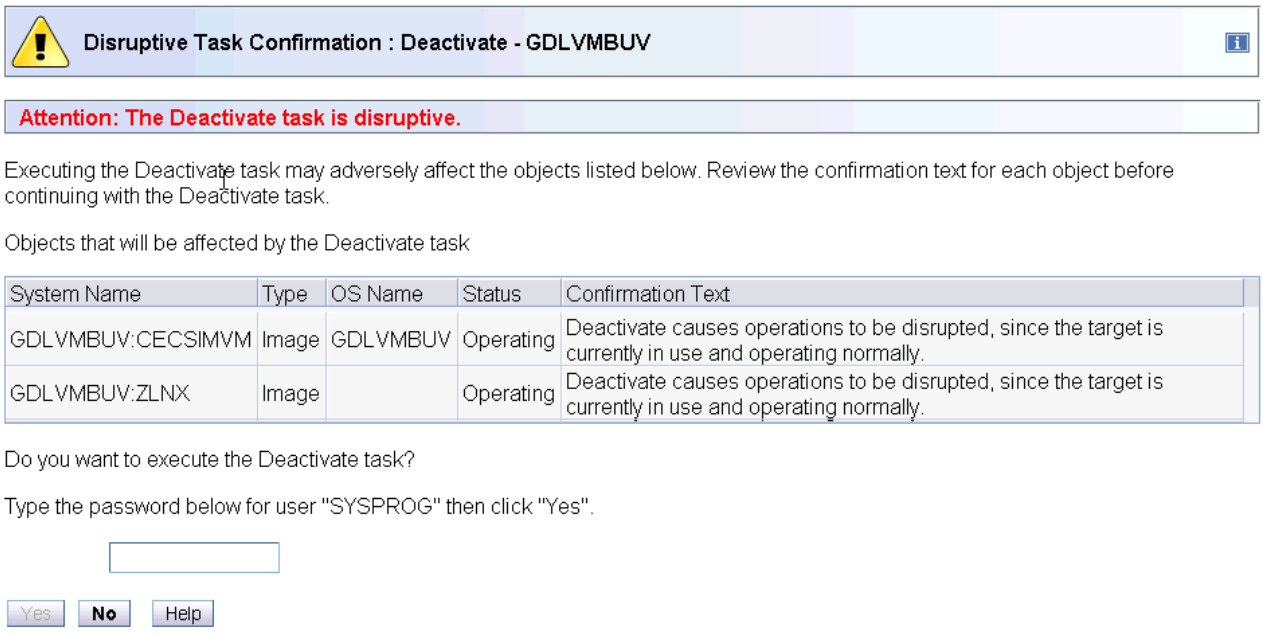


Figure 5. Disruptive task confirmation window

Depending on your user ID, you might not be able to perform the task on the selected object unless you provide required confirmation text or a required password. See the **Disruptive Task Confirmation** task help if you need additional information for this task confirmation window.

Notes:

- For tasks that are performed by using the **Single Object Operation** task, the password that is used for the Disruptive Task Confirmation window depends on if the user ID that was used to log on to the Hardware Management Console is also defined on the Support Element when the **Single Object Operation** task is used. If the user ID also exists on the Support Element, then the password must match the one for the user on the Support Element. If the user ID does not exist on the Support Element, then the password must match the one for the user ID on the Hardware Management Console.
- It is possible that the access administrator did not assign a password requirement for a particular user ID (set by the access administrator in the **User Management** task). In this case, the password input field does not display for that user ID.
- The default SERVICE user ID must always provide a password to proceed with a disruptive task.

USB flash memory drive

The USB flash memory drive is a removable writable media available on the Hardware Management Console. There can be more than one USB flash memory drive inserted into the console at one time.

Note: If you are running a task that accesses a USB flash memory drive make sure that you are accessing the correct USB flash memory drive for your task.

When you are using a task that requires reading from or writing to removable media, "USB flash memory drive" on page 14 displays a possible Select Media Device task window.

Note: If you are using systems prior to IBM z15™ (z15™), a CD/DVD-ROM can still be an acceptable media device.

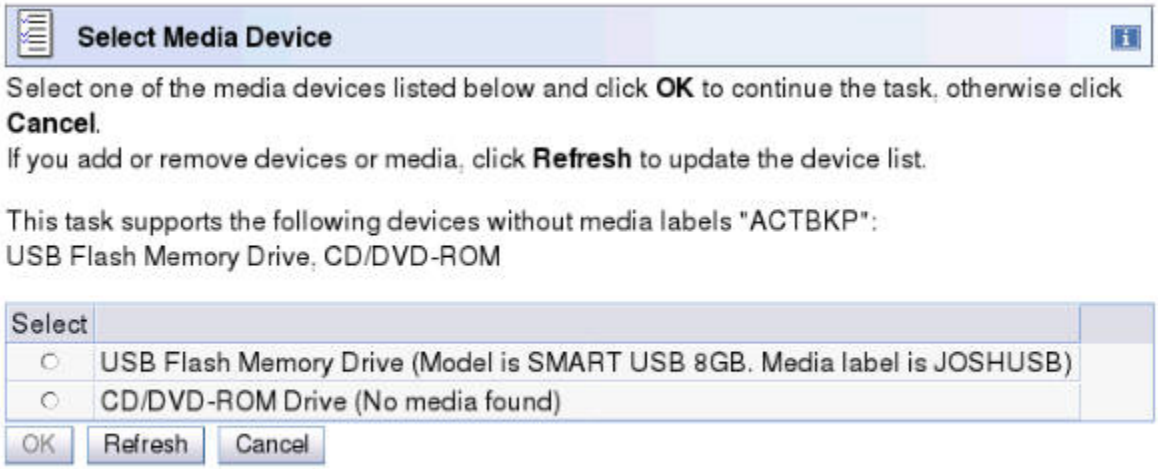


Figure 6. Select media device window

The Hardware Management Console Version 2.12.0 no longer supports a diskette or DVD-RAM media. The available media is USB flash memory drive and CD/DVD-ROM (if one exists).

Notes:

- If you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. If the media is not inserted properly, the console does not beep three times and a message is displayed indicating the drive was not added. You need to remove the device and try again.

- Tested virtual file allocation table (VFAT) and second extended file system (EXT2) USB flash memory drives, include IBM packaged SMART drives.
- Only the media that has been supplied by IBM or was formatted on the Hardware Management Console or Support Element should be used in the console.

USB flash memory drive alternatives

There are times when you may not want to use a USB flash memory drive or you cannot use read/write media. The following table lists the tasks that use the USB flash memory drive and identifies a USB flash memory drive alternative the task supports.

Table 3. USB flash memory drive alternatives

Task Name	USB Flash Memory Drive Alternative
Audit and Log Management	FTP server
Change Console Internal Code	Read only media option (feature code 0845), FTP server
Channel PCHID Assignment	Use print screen
Cryptographic Configuration (UDX Import)	CD/DVD-ROM (if available)
Export/Import Profile Data	Use HMC hard drive
FCP Configuration	FTP server
Format Media	Not applicable
Input/Output (I/O) Configuration	FTP server, use HMC hard drive
Load from File	CD/DVD-ROM (if available)
Load from Removable Media or Server	FTP server, CD/DVD-ROM (if available)
Manage Print Screen Files	Transmit service data, remotely download image files
Migrate Channel Configuration Files	CD/DVD-ROM (if available)
Nondisruptive Hardware Change	CD/DVD-ROM (if available)
Offload Problem Analysis Data to Removable Media	Transmit service data
OSA Advanced Facilities	FTP server
Perform a Repair Action	CD/DVD-ROM (if available)
Perform Model Conversion	CD/DVD-ROM (if available)
Save/Restore Customizable Console Data	Use HMC data replication
Save Upgrade Data	FTP server
System Input/Output Configuration Analyzer	FTP server
Transmit Service Data	FTP server, Transmit to Remote Support Facility (RSF)
Transmit Vital Product Data	Send to your service representative
View Security Logs	FTP server, CD/DVD-ROM (if available)

Server requirements for supporting FTP, SFTP, or FTPS

Use the following guidelines for a Linux® operating system server supporting FTP, SFTP, or FTPS.

FTP (File Transfer Protocol)

- Recommend vsftpd 2.0 or higher
- Server must support passive FTP data transfers
- Client firewalls may need to be configured to allow the passive data connection to occur

SFTP (SSH File Transfer Protocol)

- Recommend openssh 4.4 or higher
- Only user name and password client authentication is currently supported
- Client key authentication is not supported

FTPS (FTP Secure)

- Recommend vsftpd 2.0 or higher
- Server must support passive FTP data transfers
- Server must support explicit FTPS connections
- Client firewalls may need to be configured to allow the passive data connection to occur

Audit, Event, and Security Log Messages

Log messages

The log messages included in this section can be applicable to the following consoles:

- IBM Z Hardware Management Console (HMC) and Support Element (SE)
- IBM LinuxONE (LinuxONE) Hardware Management Console (HMC) and Support Element (SE)
- Trusted Key Entry (TKE) workstation

The following log messages are new for Version 2.16.0:

- “814” on page 60
- “815” on page 60
- “816” on page 60
- “817” on page 60
- “818” on page 60
- “819” on page 60
- “1065” on page 83
- “1267” on page 91
- “2102” on page 187
- “2103” on page 187
- “2104” on page 187
- “2105” on page 187
- “2106” on page 187
- “2107” on page 187
- “2108” on page 188
- “2109” on page 188
- “3000” on page 188
- “3001” on page 188
- “3002” on page 188

- “3003” on page 188
- “3322” on page 190
- “4102” on page 191
- “4103” on page 191
- “5845” on page 248
- “5846” on page 248
- “5847” on page 248
- “5970” on page 253
- “6100” on page 257
- “6101” on page 257
- “6126” on page 258
- “6127” on page 258
- “6128” on page 258
- “6129” on page 259
- “6130” on page 259
- “6131” on page 259
- “6134” on page 259
- “6135” on page 260
- “6136” on page 260
- “6137” on page 260
- “6138” on page 260
- “6150” on page 262
- “6151” on page 262
- “6152” on page 262
- “6153” on page 262
- “6154” on page 262
- “6155” on page 262
- “6165” on page 263
- “6166” on page 263
- “6167” on page 263
- “6168” on page 263
- “6169” on page 263
- “6170” on page 263
- “6171” on page 263
- “6172” on page 264
- “6173” on page 264
- “6174” on page 264
- “6175” on page 264
- “6176” on page 264
- “6177” on page 264
- “6178” on page 265
- “6179” on page 265
- “6180” on page 265

- “6181” on page 265
- “6182” on page 265
- “6184” on page 265
- “6185” on page 266
- “6186” on page 266
- “6187” on page 266
- “6188” on page 266
- “6189” on page 266
- “6190” on page 266
- “6191” on page 267
- “6192” on page 267
- “6193” on page 267
- “6194” on page 267
- “6195” on page 267
- “6196” on page 268
- “6197” on page 268
- “6198” on page 268
- “6199” on page 268
- “6200” on page 268
- “7000” on page 269
- “7001” on page 269
- “7002” on page 269

Messages 1-100

1	**Start was requested.**
2	**Stop was requested.**
3	**Multisystem channel communication unit 0 power-on reset has occurred.**
4	**Multisystem channel communication unit 1 power-on reset has occurred.**
5	**Multisystem channel communication unit 2 power-on reset has occurred.**
6	**Multisystem channel communication unit 3 power-on reset has occurred.**
7	**Multisystem channel communication unit (MCCU) 0 diagnostic power-on reset occurred.**
8	**Multisystem channel communication unit (MCCU) 1 diagnostic power-on reset occurred.**
9	**Multisystem channel communication unit (MCCU) 2 diagnostic power-on reset occurred.**
10	**Multisystem channel communication unit (MCCU) 3 diagnostic power-on reset occurred.**
11	**Processing unit is powered on.**
12	**Processing unit is powered off.**
13	**Load was successful for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

14	**Load failure occurred for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

15	**Load was cancelled for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

16	**System check.**
17	**A scheduled operation started.**
18	**Input/output (I/O) processor power-on reset has ended.**
19	**Activation has started.**
20	**Deactivation has started.**
21	**Power-on reset was started.**
22	**Channel power-on reset was started.**
23	**Input/output (I/O) processor power-on reset was started.**
24	**Battery operated clock old time.**
25	**Battery operated clock new time.**
26	**Manual problem analysis was started.**
27	**Automatic problem analysis was started.**
28	**The following internal code fixes were activated: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCF control file name

29	**The following internal code fixes were deactivated: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCF control file name

30	**The following internal code changes were installed: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCF control file name

31	**The following internal code changes were activated: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCF control file name

32	**The following internal code changes were removed: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCF control file name

33	**The following internal code changes were accepted: *{0}*.**

Explanation

Substitution variables are:

*{0}*EC number and MCL level of the change

34	**An internal code change failure occurred.**
35	**System exerciser was started.**
36	**System exerciser has ended.**
37	**A logon occurred in service representative mode.**
38	**A logon occurred in product engineering mode.**
39	**A load will be attempted for system *{0}* with the following options: type *{1}*, store status *{4}*, address *{2}*, parameter *{3}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Load type
*{2}*Load address
*{3}*Load parameter
*{4}*Load store status value

40	**A logoff occurred.**
41	**Manual problem analysis has ended.**
42	**Automatic problem analysis has ended.**
43	**Problem analysis results were displayed to the customer.**
44	**Problem analysis service information was transmitted to the Service Support System.**
45	**Machine check recovery was started.**
46	**Machine check recovery has ended.**
47	**Multisystem channel communication unit 0 diagnostics ran successfully.**
48	**Multisystem channel communication unit 1 diagnostics ran successfully.**
49	**Multisystem channel communication unit 2 diagnostics ran successfully.**
50	**Multisystem channel communication unit 3 diagnostics ran successfully.**
51	**The console application was initialized.**
52	**The Hardware Management Console Application (HWMCA) console was disabled.**
53	**Storage device or tape adapter customization change request.**
54	**Storage device or tape adapter customization change request.**
55	**Workstation adapter customization change request.**

56	**Workstation adapter customization change request.**
57	**S/370 channel customization change request.**
58	**Input/output (I/O) communication adapter customization change request.**
59	**Input/output (I/O) communication adapter customization change request.**
60	**Input/output (I/O) communication adapter customization change request.**
61	**ASCII adapter customization change request.**
62	**IEEE 802.3 adapter customization change request.**
64	**Transmission Control Protocol/Internet Protocol (TCP/IP) customization change request.**
65	**Request for price quotation adapter customization change request.**
66	**Request for price quotation adapter customization change request.**
67	**Request for price quotation adapter customization change request.**
68	**Request for price quotation adapter customization change request.**
69	**Request for price quotation adapter customization change request.**
70	**Input/output (I/O) adapter customization change request.**
71	**Input/output (I/O) adapter customization change request.**
72	**Input/output (I/O) adapter customization change request.**
73	**Input/output (I/O) adapter customization change request.**
74	**Input/output (I/O) adapter customization change request.**
75	**Input/output (I/O) adapter customization change request.**
76	**Redundant bit was set.**
77	**Backup battery power is active.**
78	**Power is restored.**
79	**Remote console was invoked.**
80	**Operations management is active.**
81	**User profile *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*User profile name

82	**User profile *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*User profile name

83	**The vital product data was rebuilt.**
84	**A request to send configuration data to the Service Support System was put on the remote support queue.**
85	**Configuration data and vital product data were restored from diskette.**
86	**An upgrade installation operation was started.**

87	**Configuration data was changed to an edit operation.**
88	**An input/output (I/O) controller was power-on reset.**
89	**An input/output (I/O) controller was power-on reset.**
90	**An input/output (I/O) controller was power-on reset.**
91	**An input/output (I/O) controller was power-on reset.**
92	**An input/output (I/O) controller was power-on reset.**
93	**An input/output (I/O) controller was power-on reset.**
94	**An input/output (I/O) controller was power-on reset.**
95	**An input/output (I/O) controller was power-on reset.**
96	**An input/output (I/O) controller was power-on reset.**
97	**An input/output (I/O) controller was power-on reset.**
98	**An input/output (I/O) controller was power-on reset.**
99	**An input/output (I/O) controller was power-on reset.**
100	**An input/output (I/O) controller was power-on reset.**

Messages 101-200

101	**An input/output (I/O) controller was power-on reset.**
102	**An input/output (I/O) controller was power-on reset.**
103	**An input/output (I/O) controller was power-on reset.**
104	**An input/output (I/O) controller was power-on reset.**
105	**An input/output (I/O) controller was power-on reset.**
106	**An input/output (I/O) controller was power-on reset.**
107	**An input/output (I/O) controller was power-on reset.**
108	**An input/output (I/O) controller was power-on reset.**
109	**An input/output (I/O) controller was power-on reset.**
110	**An input/output (I/O) controller was power-on reset.**
111	**Activation was successful.**
112	**Activation has failed.**
113	**Deactivation was successful.**
114	**Deactivation has failed.**
115	**The *{1}* profile *{0}* was created.**

Explanation

Substitution variables are:

*{0}*Profile name
*{1}*Profile type

116	**The *{1}* profile *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*Profile name
*{1}*Profile type

117	**The *{1}* profile *{0}* was upgraded.**

Explanation

Substitution variables are:

*{0}*Profile name
*{1}*Profile type

118	**The *{1}* profile *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*Profile name
*{1}*Profile type

119	**A scheduled operation completed successfully.**
120	**A scheduled operation failed.**
121	**A scheduled operation was added.**
122	**A scheduled operation was attempted but did not start.**
123	**A logon occurred in operator mode.**
124	**A logon occurred in advanced operator mode.**
125	**A logon occurred in access administrator mode.**
126	**A logon occurred in system programmer mode.**
127	**Setup installation options operation started.**
128	**Setup installation options operation ended.**
129	**The keylock position is secure.**
130	**The keylock position is manual.**
131	**The keylock position is normal.**
132	**The keylock position is auto.**
133	**Internal code change was retrieved.**
134	**Uninterruptible power supply (UPS) battery is active.**
135	**Processor battery is active.**
136	**Local unsuccessful logon detected.**
137	**Operations management unsuccessful logon detected.**
138	**Remote operations unsuccessful logon detected.**
139	**An automatic dial attempt was made.**
140	**A manual dial attempt was made.**
141	**A call attempt was successful.**
142	**A call attempt was not successful.**
143	**A failure alert was generated.**
144	**Failure alert information was transmitted to the central site.**

145	**Events in the event log were deleted.**
146	**Due to event log space limitations, obsolete events were deleted.**
147	**A remote console session terminated successfully from system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

148	**A remote console session terminated with an error condition from system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

149	**Line disconnect key was requested.**
150	**A remote connection was attempted.**
151	**A remote connection failed.**
152	**A remote connection was successful.**
153	**Automatic activation was enabled.**
154	**Automatic activation was disabled.**
155	**Multisystem channel communication unit 0 successfully installed.**
156	**Multisystem channel communication unit 1 successfully installed.**
157	**Multisystem channel communication unit 2 successfully installed.**
158	**Multisystem channel communication unit 3 successfully installed.**
159	**Multisystem channel communication unit 0 successfully removed.**
160	**Multisystem channel communication unit 1 successfully removed.**
161	**Multisystem channel communication unit 2 successfully removed.**
162	**Multisystem channel communication unit 3 successfully removed.**
163	**Multisystem channel communication unit 0 configuration changed.**
164	**Multisystem channel communication unit 1 configuration changed.**
165	**Multisystem channel communication unit 2 configuration changed.**
166	**Multisystem channel communication unit 3 configuration changed.**
167	**Write of input/output configuration data set (IOCDS) *{0}* in progress.**

Explanation

Substitution variables are:

*{0}*IOCDS identifier

168	**Stand alone build of input/output configuration data set (IOCDS) *{0}* in progress.**

Explanation

Substitution variables are:

*{0}*IOCDS identifier

169 **Diskette import of configuration source *{0}* started.**

Explanation

Substitution variables are:

*{0}*IOCDS name

170 **Tape import of configuration source *{0}* started.**

Explanation

Substitution variables are:

*{0}*IOCDS name

171 **Edit of configuration source *{0}* is in progress.**

Explanation

Substitution variables are:

*{0}*IOCDS name

172 **Disassemble of input/output configuration data set (IOCDS) *{0}* to configuration source.**

Explanation

Substitution variables are:

*{0}*IOCDS name

173 **Export of configuration source *{0}* to system tape started.**

Explanation

Substitution variables are:

*{0}*IOCDS name

174 **S/370 check stop occurred.**

175 **A scheduled operation failed to start within the specified time window.**

176 **The system clock has changed.**

177 **Cable reconnected.**

178 **Power-on reset has ended.**

179 **An automatic dial to *{0}* was attempted. The dial operation failed.**

Explanation

Substitution variables are:

*{0}*Phone number

190 **Problem analysis found, but did not report, a problem identical to an open problem.**

191 **Local unsuccessful logon threshold exceeded.**

192 **Operations management unsuccessful logon threshold exceeded.**

193 **Remote operations unsuccessful logon threshold exceeded.**

194 **The following internal code changes were deleted: *{0}*.**

Explanation

Substitution variables are:

*{0}*Engineering change numbers

195 **Problem analysis found nothing to report.**

196 **Write of input/output configuration data set (IOCDS) *{0}* in progress.**

Explanation

Substitution variables are:

*{0}*IOCDS name

197 **Stand-alone build of input/output configuration data set (IOCDS) *{0}* in progress.**

Explanation

Substitution variables are:

*{0}*IOCDS identifier

198 **Diskette import of configuration source *{0}* started.**

Explanation

Substitution variables are:

*{0}*IOCDS name

199 **Tape import of configuration source *{0}* started.**

Explanation

Substitution variables are:

*{0}*IOCDS name

200 **Edit of configuration source *{0}* is in progress.**

Explanation

Substitution variables are:

*{0}*IOCDS name

Messages 201-300

201 **Disassemble of input/output configuration data set (IOCDS) *{0}* to configuration source.**

Explanation

Substitution variables are:

*{0}*IOCDS name

202 **Export of configuration source *{0}* to system tape started.**

Explanation

Substitution variables are:

*{0}*IOCDS name

203 **An automatic dial to *{0}* was attempted. The dial operation was successful.**

Explanation

Substitution variables are:

*{0}*Telephone number

204 **S/390 check stop occurred.**

205 **A scheduled operation failed to start within the specified time window.**

206 **The system clock has changed.**

207 **Cable reconnected.**

208 **Power-on reset has ended.**

209 **Input/output (I/O) processor power-on reset for *{0}* was started on channel path identifier *{1}*.**

Explanation

Substitution variables are:

*{0}*CPC name
*{1}*CHPID type

210 **Input-output (I/O) processor power-on reset for *{0}* was completed on channel path identifier *{1}*.**

Explanation

Substitution variables are:

*{0}*CPC name
*{1}*CHPID type

211 **Customization change request for Input-output (I/O) processor *{0}* on channel path identifier *{1}*.**

Explanation

Substitution variables are:

*{0}*IOP name
*{1}*CHPID type

213 **Activation has started using the *{1}* profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Profile type
*{1}*Profile name

214 **Deactivation has started for *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

215 **An automatic dial to *{0}* was attempted. The dial operation failed.**

Explanation

Substitution variables are:

*{0}*Telephone number

216 **User *{0}* has logged on in *{1}* mode.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*User role

217 **Channel path swap completed for channels *{0}* and *{1}*.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*CHPID type

218 **Reset of swapped channel paths completed for channels *{0}* and *{1}*.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*CHPID type

219 **Channel path swap for channels *{0}* and *{1}* will be active after power-on reset.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*CHPID type

220 **Reset of swapped channel paths for channels *{0}* and *{1}* will be active after power-on reset.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*CHPID type

221 ***{0}* was made the active input/output configuration data set (IOCDS).**

Explanation

Substitution variables are:

*{0}*IOCDS identifier

222 **Input/output configuration data set (IOCDS) *{0}* written to *{1}* by *{2}*.**

Explanation

Substitution variables are:

*{0}*IOCDS name
*{1}*IOCDS identifier
*{2}*Function, such as IOCP

223 **Hardware configuration definition (HCD) data set written.**

224 **Channel path identifier *{0}* entered the reserved state.**

Explanation

Substitution variables are:

*{0}*CHPID type

225 **Channel path identifier *{0}* entered the standby state.**

Explanation

Substitution variables are:

*{0}*CHPID type

226 **Channel path identifier *{0}* entered the online state.**

Explanation

Substitution variables are:

*{0}*CHPID type

227 **Dynamic input/output (I/O) reconfiguration started.**

228 **Dynamic input/output (I/O) reconfiguration ended.**

229 **Activation started for system *{0}* using profile *{1}*.**

Explanation

Substitution variables are:

*{0}*Target name
*{1}*Profile name

230 **Activation completed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

231 **Activation failed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

232 **Deactivation started for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

233 **Deactivation completed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

234 **Deactivation failed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

235 **System reset started for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

236 **System reset completed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

237 **System reset failed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

238 **Activate request was initiated for system *{0}* using profile *{1}*.**

Explanation

Substitution variables are:

*{0}*CPC or Image name
*{1}*Profile name

239 **Activate request has ended successfully for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC or Image name

240 **Activate request has ended with failure for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC or Image name

241 **Deactivate request was initiated for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC or Image name

242 **Deactivate request has ended successfully for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC or Image name

243 **Deactivate request has ended with failure for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC or Image name

244 **System reset started for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

245 **System reset completed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

246 **System reset failed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

247 **A start operation completed on system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

248 **A start operation failed on system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

249 **A stop operation completed on system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

250 **A stop operation failed on system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

251 **A restart operation completed on system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

252 **A restart operation failed on system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

253 **Engineering change (EC) upgrade started for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

254 **Engineering change (EC) upgrade completed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

255 **Engineering change (EC) upgrade failed.**

256 **System check stop.**

257 **Logon by *{0}*.**

Explanation

Substitution variables are:

*{0}*User name

258	**Logoff.**
259	**Load successful *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

260	**Power-on successful.**
261	**Power-off started.**
262	**System reset successful.**
263	**Battery operated clock was set.**
264	**Activate successful *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

265	**Deactivate successful *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

266	**Midnight at processor controller.**
267	**Expanded storage in check stopped state.**
268	**Partition *{0}* in check stopped state.**

Explanation

Substitution variables are:

*{0}*Image name

269	**Channel subsystem failure.**
270	**Central storage failure.**
271	**Expanded storage failure.**
272	**System complex (Sysplex) timer failure.**
273	**Link failure on channel path identifier (CHPID) *{0}*.**

Explanation

Substitution variables are:

*{0}*CHPID type

274	**Processor *{0}* has entered disabled wait state (PSW *{1}*).**

Explanation

Substitution variables are:

*{0}*Processor number
*{1}*PSW number

275 **Partition *{0}* processor *{1}* has entered disabled wait (PSW *{2}*).**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Processor number
*{2}*PSW number

276 **Program status word (PSW) loop not valid on processor *{0}* (*{1}*).**

Explanation

Substitution variables are:

*{0}*Processor number
*{1}*Target number

277 **Logically partitioned mode failure.**

278 **Logically partitioned mode initialization complete.**

279 **Logically partitioned mode initialization failure.**

280 **Vary Processor *{0}* command received.**

Explanation

Substitution variables are:

*{0}*Processor number

281 **Vary vector element *{0}* command received.**

Explanation

Substitution variables are:

*{0}*Vector number

282 **Processor *{0}* failed to initialize.**

Explanation

Substitution variables are:

*{0}*Processor number

283 **Processor *{0}* in check stopped state *{1}*.**

Explanation

Substitution variables are:

*{0}*Processor number
*{1}*Check stopped state

284 **CHPIDs *{0}*-*{1}* in check stopped state.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*CHPID type

285 **CHPID *{0}* deconfigured during reset *{1}*.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*Reset state

286 **Vector element *{0}* failed.**

Explanation

Substitution variables are:

*{0}*Vector number

287 **Physical processor *{0}* logically check stopped.**

Explanation

Substitution variables are:

*{0}*Processor name

288 **Time of day (TOD) clock failure.**

289 **Cryptographic feature failure *{0}*.**

Explanation

Substitution variables are:

*{0}*Failure reason

290 **Dynamic storage access link failure.**

291 **Processor controller error occurred.**

292 **Service processor damage machine check occurred.**

293 **Cryptographic feature sensor activated.**

294 **Operator console not operational *{0}*.**

Explanation

Substitution variables are:

*{0}*Console name

295 **Call authorization requested.**

296 **Outbound remote support call started.**

297 **Outbound remote support call delayed for *{0}* hours.**

Explanation

Substitution variables are:

*{0}*Number of hours

298 **Service call accepted, support group notified.**

299 **Remote support call completed.**

300 **Remote support call failed.**

Messages 301-400

301 **Remote support call cancelled.**

302 **Power-off started.**

303 **Power-on reset completed.**

304 **System reset completed.**

305 **System power-on reset completed.**

306 **Transition into physically partitioned (PP) mode.**

307 **Transition into single image (SI) mode.**

308 **Vary storage range *{0}*-*{1}* megabyte command received.**

Explanation

Substitution variables are:

*{0}*Start of storage range
*{1}*End of storage range

309 **Vary storage element *{0}* command received *{1}*.**

Explanation

Substitution variables are:

*{0}*Storage element
*{1}*Command result

310 **Vary expanded storage element command received *{0}*.**

Explanation

Substitution variables are:

*{0}*Command result

311 **Vary channel path command received *{0}*.**

Explanation

Substitution variables are:

*{0}*Command result

312 **Vary channel set *{0}* channel number *{1}* command received *{2}*.**

Explanation

Substitution variables are:

*{0}*Channel set
*{1}*Channel number
*{2}*Command result

313 **Command completed. Response code: *{0}*.**

Explanation

Substitution variables are:

*{0}*Response code number

314 **Hardware element configured on: *{0}*.**

Explanation

Substitution variables are:

*{0}*Hardware element

315 **Hardware element configured off: *{0}*.**

Explanation

Substitution variables are:

*{0}*Hardware element

316 **Central storage configured on: *{0}*-*{1}*.**

Explanation

Substitution variables are:

*{0}*Start of storage range
*{1}*End of storage range

317 **Central storage configured off: *{0}*-*{1}*.**

Explanation

Substitution variables are:

*{0}*Start of storage range
*{1}*End of storage range

318 **Expanded storage configured on: *{0}*-*{1}*.**

Explanation

Substitution variables are:

*{0}*Start of storage range
*{1}*End of storage range

319 **Expanded storage configured off: *{0}*-*{1}*.**

Explanation

Substitution variables are:

*{0}*Start of storage range
*{1}*End of storage range

320 **Power or thermal system failure.**

321 **Critical power or thermal fault.**

322 **Logout analysis disabled.**

323 **Load failed *{0}*.**

Explanation

Substitution variables are:

*{0}*Processor number

324 **Load cancelled *{0}*.**

Explanation

Substitution variables are:

*{0}*Processor number

325 **Load rejected *{0}*.**

Explanation

Substitution variables are:

*{0}*Processor number

326 **Power on failed.**

327 **Power on cancelled.**

328 **Power on rejected.**

329 **System reset failed.**

330 **System reset cancelled.**

331 **System reset rejected.**

332 **Activate failed *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

333 **Activate cancelled *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

334 **Activate rejected *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

335 **Deactivate failed *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

336 **Deactivate cancelled *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

337 **Deactivate rejected *{0}*.**

Explanation

Substitution variables are:

*{0}*Target name

338 **CHPID *{0}* in check stopped state.**

Explanation

Substitution variables are:

*{0}*338

339 **Vector element failed *{0}*.**

Explanation

Substitution variables are:

*{0}*Vector name

340 **Invalid PSW loop on processor *{0}*.**

Explanation

Substitution variables are:

*{0}*Processor number

341 **Processor *{0}* in check stopped state.**

Explanation

Substitution variables are:

*{0}*Processor number

342 **CHPID *{0}* deconfigured during reset.**

Explanation

Substitution variables are:

*{0}*CHPID type

343 **Vector element failed.**

344 **Crypto failure.**

345 **Operator console not operational.**

346 **Vary storage element *{0}* command received.**

Explanation

Substitution variables are:

*{0}*Storage element

347 **Vary expanded storage element command received.**

348 **Vary channel path command received.**

349 **Vary channel set *{0}* channel number *{1}* command received.**

Explanation

Substitution variables are:

*{0}*Channel set
*{1}*Channel number

350 **CHPIDs *{0}*-*{1}* deconfigured during reset *{2}*.**

Explanation

Substitution variables are:

*{0}*Start CHPID range
*{1}*End CHPID range
*{2}*Target name

351 **CHPIDs *{0}*-*{1}* deconfigured during reset.**

Explanation

Substitution variables are:

*{0}*Start CHPID range
*{1}*End CHPID range

352 **Partition *{2}*: CHPIDs *{0}* and *{1}* in check stopped state.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*CHPID type
*{2}*CHPID type

353 **Processor *{0}* has entered disabled wait state.**

Explanation

Substitution variables are:

*{0}*Processor number

354 **Automatic activation has started using the *{1}* profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Profile type
*{1}*Profile name

355	**System activity analysis started.**
356	**System activity analysis ended.**
358	**DCAF attempt rejected: DCAF target program is already active with another DCAF session.**
359	**DCAF session ended.**
360	**User DCAF attempt rejected: ROF disabled or user is logged on.**
361	**PE DCAF attempt rejected: user is logged on.**
362	**DCAF attempt rejected: ROF is currently active.**
363	**DCAF attempt rejected: Bad password used.**

Messages 401-500

479	**S370 channel RPQ was successful.**
480	**S370 channel RPQ failed.**
481	**Undo S370 channel RPQ was successful.**
482	**Undo S370 channel RPQ failed.**
483	**The following operation was cancelled: *{0}*. It was scheduled by *{1}* from *{2}* on *{3}*.**

Explanation

Substitution variables are:

*{0}*Description of the operation
*{1}*User name
*{2}*NAU
*{3}*Creation date

497	**The following operation was scheduled by *{1}* from *{2}*: *{0}*.**

Explanation

Substitution variables are:

*{0}*Description of the operation
*{1}*User name
*{2}*NAU

498	**The following operation started: *{0}*. It was scheduled by *{1}* from *{2}* on *{3}*.**

Explanation

Substitution variables are:

*{0}*Description of the operation
*{1}*User name
*{2}*NAU
*{3}*Creation date

499	**The following operation failed to start within the specified time window: *{0}*. It was scheduled by *{1}* from *{2}* on *{3}*.**

Explanation

Substitution variables are:

*{0}*Description of the operation
*{1}*User name
*{2}*NAU
*{3}*Creation date

500 **The following operation was attempted but did not start: *{0}*. It was scheduled by *{1}* from *{2}*.*{3}* on *{4}*.**

Explanation

Substitution variables are:

*{0}*Description of the operation
*{1}*User name
*{2}*NetId
*{3}*NAU
*{4}*Creation date

Messages 501-600

501 **The following operation was attempted but failed: *{0}*. It was scheduled by *{1}* from *{2}* on *{3}*.**

Explanation

Substitution variables are:

*{0}*Description of the operation
*{1}*User name
*{2}*NAU
*{3}*Creation date

502 **The following disruptive operation started: *{0}*. It was requested from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Disruptive operation
*{1}*Network ID
*{2}*NAU

503 **The following disruptive operation started: *{0}*. It was requested by *{1}* from *{2}*.*{3}*.**

Explanation

Substitution variables are:

*{0}*Disruptive operation
*{1}*User name
*{2}*Network ID
*{3}*NAU

504 **Engineering change (EC) information query for concurrency status started for system *{0}*.**

Explanation

Substitution variables are:

*{0}*System name

505	**Engineering change (EC) information query for concurrency status completed.**
512	**A scheduled operation started.**
513	**A scheduled operation completed successfully.**
514	**A scheduled operation failed.**
515	**A scheduled operation failed to start within the specified time window.**
516	**A scheduled activate failed to start within the specified time window.**
517	**A scheduled deactivate failed to start within the specified time window.**
518	**A scheduled retrieve of internal code changes failed to start within the specified time window.**
519	**A scheduled install of internal code changes failed to start within the specified time window.**
520	**A scheduled hard disk backup failed to start within the specified time window.**
521	**A scheduled remove of internal code changes failed to start within the specified time window.**
522	**User *{0}* attempted to log on with a user identification or password that was not valid.**

Explanation

Substitution variables are:

*{0}*User name

523	**A remote console session was initiated with system *{0}*.**

Explanation

Substitution variables are:

*{0}*System name

524	**Concurrent internal code changes for I390/PU started.**
525	**Concurrent internal code changes for I390/PU completed.**
526	**Concurrent internal code changes for I390/PU failed.**
527	**Concurrent internal code changes for I390/PU completed with no changes required for current operating mode.**
528	**A scheduled accept of internal code changes failed to start within the specified time window.**
529	**A scheduled install and activate of internal code changes failed to start within the specified time window.**
530	**A scheduled retrieve and install of internal code changes failed to start within the specified time window.**
531	**A scheduled set clock operation failed to start within the specified time window.**
532	**A scheduled power on failed to start within the specified time window.**
533	**A scheduled power off failed to start within the specified time window.**
534	**A scheduled load failed to start within the specified time window.**
535	**A scheduled system reset failed to start within the specified time window.**
536	**A scheduled clock synchronization failed to start within the specified time window.**

537	**A scheduled operation was attempted but did not start.**
538	**Concurrent internal code changes for PR/SM started.**
539	**Concurrent internal code changes for PR/SM completed.**
540	**Concurrent internal code changes for PR/SM failed.**
541	**Concurrent internal code changes for CFCC started.**
542	**Concurrent internal code changes for CFCC completed.**
543	**Concurrent internal code changes for CFCC failed.**
544	**A scheduled activate was attempted but did not start.**
545	**A scheduled deactivate was attempted but did not start.**
546	**A scheduled retrieve of internal code changes was attempted but did not start.**
547	**A scheduled install of internal code changes was attempted but did not start.**
548	**A scheduled hard disk backup was attempted but did not start.**
549	**A scheduled remove of internal code changes was attempted but did not start.**
550	**A scheduled accept of internal code changes was attempted but did not start.**
551	**A scheduled install and activate of internal code changes was attempted but did not start.**
552	**A scheduled retrieve and install of internal code changes was attempted but did not start.**
553	**A scheduled set clock operation was attempted but did not start.**
560	**A scheduled power on was attempted but did not start.**
561	**A scheduled power off was attempted but did not start.**
562	**A scheduled load was attempted but did not start.**
563	**A scheduled system reset was attempted but did not start.**
564	**A scheduled clock synchronization was attempted but did not start.**
565	**The following internal code changes were retrieved from diskette: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCL levels

566	**The following internal code changes were retrieved from mass storage media: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCL levels

567	**The following internal code changes were requested to be retrieved from the support system: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCL levels

568 **The following internal code changes were retrieved from the server: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCL levels

569 **A failure occurred activating the following internal code fixes: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCF control file name

575 **A failure occurred activating internal code changes.**

576 **A failure occurred deactivating the following internal code fixes: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCF control file name

577 **A failure occurred retrieving the following internal code changes: *{0}*.**

Explanation

Substitution variables are:

*{0}*Message describing the failure.

578 **A failure occurred installing the following internal code changes: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCL levels

579 **A failure occurred activating the following internal code changes: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCL levels

581 **A failure occurred removing the following internal code changes: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCL levels

582 **A failure occurred deleting the following internal code changes: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCL levels

583 **A failure occurred accepting the following internal code changes: *{0}*.**

Explanation

Substitution variables are:

*{0}*MCL levels

586 **Retrieve internal code changes started by an automatic operations command from a central control host.**

587 **Retrieve internal code changes, started by an automatic operations command from a central control host, completed.**

590 **Communications are not active between this console and the console named *{0}*.**

Explanation

Substitution variables are:

*{0}*HMC console name

591 **Communications are not active between the Hardware Management Console and the Support Element for system *{0}*.**

Explanation

Substitution variables are:

*{0}*SE console name

Messages 601-700

614 **Activation of any existing internal code changes has started.**

615 **Coupling facility control code load started.**

616 **Coupling facility control code load completed successfully.**

617 **Coupling facility control code load failed.**

618 **Deactivate and delete of all temporary internal code fixes started for system *{0}*.**

Explanation

Substitution variables are:

*{0}*System name

619 **Deactivate and delete of all temporary internal code fixes completed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*System name

620 **Deactivate and delete of all temporary internal code fixes failed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*System name

621 **Retrieve internal code changes initiated by a central control host has started.**

622	**Retrieve internal code changes initiated by a central control host has completed.**
623	**Settings saved automatically to not allow installation and activation of internal code changes.**
624	**Settings saved on Hardware Management Console *{0}* to allow installation and activation of internal code changes.**

Explanation

Substitution variables are:

*{0}*Origin HMC

625	**Settings saved manually on Hardware Management Console *{0}* to not allow installation and activation of internal code changes.**

Explanation

Substitution variables are:

*{0}*Origin HMC

626	**A scheduled transmit system availability data failed to start within the specified time window.**
627	**A scheduled transmit system availability data was attempted, but did not start.**
628	**Concurrent internal code changes for channels started.**
629	**Concurrent internal code changes for channels completed.**
630	**Concurrent internal code changes for channels failed.**
631	**Concurrent internal code changes for a supported storage subsystem's device drives started.**
632	**Concurrent internal code changes for a supported storage subsystem's device drives completed.**
633	**Concurrent internal code changes for a supported storage subsystem's device drives failed.**
634	**Concurrent internal code changes for cage controller started.**
635	**Concurrent internal code changes for cage controller completed.**
636	**Concurrent internal code changes for cage controller failed.**
637	**Concurrent internal code changes for power started.**
638	**Concurrent internal code changes for power completed.**
639	**Concurrent internal code changes for power failed.**
640	**Concurrent internal code changes for Support Element started.**
641	**Concurrent internal code changes for Support Element completed.**
642	**Concurrent internal code changes for Support Element failed.**
658	**Concurrent internal code changes started.**
659	**Concurrent internal code changes completed.**
660	**Concurrent internal code changes failed.**
661	***{0}*.**

Explanation

Service require state message.

Substitution variables are:

*{0}*A message describing the reason service required state was turned on or a message saying service required state was turned off.

662	**Backup critical data started.**
663	**Backup critical data ended.**
664	**Configuration data was copied to a diskette.**
665	**Configuration data was copied to the Hardware Management Console hard disk.**
666	**The system console was initialized.**
667	**The central processor complex (CPC) console was disabled.**
668	**Concurrent internal code changes initiated by MCL process.**
669	**Concurrent internal code changes initiated by pedebug panel.**
670	**Concurrent internal code changes initiated by systemTst testcase.**
671	**Activation starting load delay for power sequencing of *{0}* seconds.**

Explanation

Substitution variables are:

*{0}*Load delay seconds

672	**Activation ending load delay for power sequencing of *{0}* seconds.**

Explanation

Substitution variables are:

*{0}*Load delay seconds

673	**Starting remote support call *{1}* for console *{0}*. Type: *{2}*.**

Explanation

Substitution variables are:

*{0}*Console name and IP address
*{1}*Date and time
*{2}*Description

674	**Remote support call generated on *{1}* completed successfully by server *{0}*.**

Explanation

Substitution variables are:

*{0}*Call home server
*{1}*Rsf requestor

675	**Remote support call generated on *{1}* cancelled at server *{0}*.**

Explanation

Substitution variables are:

*{0}*Call home server
*{1}*Rsf requestor

676 **Remote support call generated on *{1}* failed at server *{0}*. Reason: Internal code error.**

Explanation

Substitution variables are:

*{0}*Call home server
*{1}*Rsf requestor

677 **Remote support call generated on *{1}* failed at server *{0}*. Reason: No phone number available.**

Explanation

Substitution variables are:

*{0}*Call home server
*{1}*Rsf requestor

678 **Remote support call generated on *{1}* failed at server *{0}*. Reason: Connectivity failed.**

Explanation

Substitution variables are:

*{0}*Call home server
*{1}*Rsf requestor

679 **Remote support call generated on *{1}* failed at server *{0}*. Reason: Remote support returned an error.**

Explanation

Substitution variables are:

*{0}*Call home server
*{1}*Rsf requestor

680 **Remote support call generated on *{1}* failed at server *{0}*. Reason: Machine is not registered.**

Explanation

Substitution variables are:

*{0}*Call home server
*{1}*Rsf requestor

681 **Remote support call generated on *{1}* failed at server *{0}*. Reason: Probable connectivity failure.**

Explanation

Substitution variables are:

*{0}*Call home server
*{1}*Rsf requestor

682 **Remote support call generated on *{1}* failed at server *{0}*. Reason: Device type not supported.**

Explanation

Substitution variables are:

*{0}*Call home server
*{1}*Rsf requestor

683 **A zeroize was performed against crypto element *{0}*. The Crypto Module Identifier (CMID) of the processor is: *{1}*.**

Explanation

Substitution variables are:

*{0}*Crypto number
*{1}*Crypto module identifier

684 **An import was performed against crypto element *{0}*. The Crypto Module Identifier (CMID) of the processor is: *{1}*.**

Explanation

Substitution variables are:

*{0}*Crypto number
*{1}*Crypto module identifier

685 **Installing internal code changes was attempted, but there were no changes to install.**

686 **Removing internal code changes was attempted, but there were no changes to remove.**

687 **User *{0}* was logged on automatically at the console.**

Explanation

Substitution variables are:

*{0}*User name

688 **Model conversion started**

689 **Model conversion completed successfully.**

690 **Model conversion failed.**

691 **The following operation was scheduled by *{1}* from *{2}.{3}* at IP address *{4}*: *{0}*.**

Explanation

Substitution variables are:

*{0}*Object name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*IP address

692 **The following operation started: *{0}*. It was scheduled by *{1}* from *{2}.{3}* at IP address *{4}* on *{5}*.**

Explanation

Substitution variables are:

*{0}*Operation name

*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*IP address
*{5}*Network ID

693 **The following operation failed to start within the specified time window: *{0}*. It was scheduled by *{1}* from *{2}.{3}* at IP address *{4}* on *{5}*.**

Explanation

Substitution variables are:

*{0}*Operation name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*IP address
*{5}*Network ID

694 **The following operation was attempted but did not start: *{0}*. It was scheduled by *{1}* from *{2}.{3}* at IP address *{4}* on *{5}*.**

Explanation

Substitution variables are:

*{0}*Operation name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*IP address
*{5}*Network ID

695 **The following operation was attempted but failed: *{0}*. It was scheduled by *{1}* from *{2}.{3}* at IP address *{4}* on *{5}*.**

Explanation

Substitution variables are:

*{0}*Operation name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*IP address
*{5}*Network ID

696 **The following operation was cancelled: *{0}*. It was scheduled by *{1}* from *{2}.{3}* at IP address *{4}* on *{5}*.**

Explanation

Substitution variables are:

*{0}*Operation name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU

*{4}*IP address
*{5}*Network ID

697 **The following disruptive operation started: *{0}*. It was requested by *{1}* from *{2}*.*{3}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Operation name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*IP address

Messages 701-800

701 **Battery operated clock set to new time obtained from *{0}*.**

Explanation

Substitution variables are:

*{0}*Network ID.NAU

702 **Activation profiles were imported.**

703 **System activity profiles were imported.**

704 **Activation profiles were exported.**

705 **System activity profiles were exported.**

706 **Model conversion to model *{0}* completed successfully.**

Explanation

Substitution variables are:

*{0}*Model number

707 **Changed write protect of Input/Output Configuration Data Set (IOCDS) *{0}* in *{1}* to *{2}*.**

Explanation

Substitution variables are:

*{0}*IOCDS name
*{1}*IOCDS identifier
*{2}*Function, such as IOCP

708 **Failed writing Input/Output Configuration Data Set (IOCDS) *{0}* to *{1}* by *{2}*.**

Explanation

Substitution variables are:

*{0}*IOCDS name
*{1}*IOCDS identifier
*{2}*Function, such as IOCP

709 **User profile *{0}* was created.**

Explanation

Substitution variables are:

*{0}*User profile name

710	**Memory upgrade completed successfully.**
711	**Memory upgrade failed.**
712	**An LPAR Dump, initiated by *{0}*, has been taken.**

Explanation

Substitution variables are:

*{0}*User name

713	**CHPID *{0}* was released.**

Explanation

Substitution variables are:

*{0}*CHPID type

714	**ID *{0}* was reassigned from logical partition *{1}* to logical partition *{2}*.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*Old image name
*{2}*New image name

715	**The power save state started.**
716	**The power save state ended.**
717	**Display/alter was used to: *{0} {1} {2}*.**

Explanation

Substitution variables are:

*{0}*Display or alter
*{1}*Image and CP names
*{2}*Display/alter function

718	**Logical partition control settings were changed.**
719	**Logical partition security settings were changed.**
720	**Logical partition cryptographic control settings were changed.**
721	**A backup of critical data was performed.**
722	**An upgrade to EC level *{0}* was performed.**

Explanation

Substitution variables are:

*{0}*EC level

723 **Remote support call generated on *{1}* failed at server *{0}*. It will be attempted at another server if available.**

Explanation

Substitution variables are:

*{0}*Handling machine name
*{1}*Origin machine name

724 **The Support Element was upgraded to *{0}* EC level by *{1}*.**

Explanation

Substitution variables are:

*{0}*EC level
*{1}*Network ID.NAU

725 **The *{1}* profile *{0}* was imported.**

Explanation

Substitution variables are:

*{0}*Profile type
*{1}*Profile name

726 **An attempt to reassign ID *{0}* failed.**

Explanation

Substitution variables are:

*{0}*CHPID type

727 **The central storage allocated to logical partition *{0}* was changed from *{1}* MB to *{2}* MB.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Old storage
*{2}*New storage

728 **The expanded storage allocated to logical partition *{0}* was changed from *{1}* MB to *{2}* MB.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Old storage
*{2}*New storage

729 **Logical processor *{0}* was configured off from logical partition *{1}*.**

Explanation

Substitution variables are:

*{0}*CP number
*{1}*Image name

730 **Logical processor *{0}* was configured on to logical partition *{1}*.**

Explanation

Substitution variables are:

*{0}*CP number
*{1}*Image name

731 **A DCAF connection to the Support Element was started in user mode *{0}*.**

Explanation

Substitution variables are:

*{0}*User name

732 **A DCAF connection to the Support Element was ended.**

733 **The security log was archived.**

734 **Remote support call generated on *{1}* is being handled by call-home server *{0}*.**

Explanation

Substitution variables are:

*{0}*Destination machine name and IP address
*{1}*Origin machine name

735 **Power on was performed.**

736 **Power off was performed.**

737 **Reset normal was performed.**

738 **Reset clear was performed.**

739 **Power-on reset started.**

740 **Power-on reset was successful.**

741 **Power-on reset was partially successful.**

742 **Power-on reset failed.**

743 **The following operation failed: *{0}*. It was scheduled by *{1}* from *{2}.{3}* on *{4}*.**

Explanation

Substitution variables are:

*{0}*Operation name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Network ID

744 **The following operation failed: *{0}*. It was scheduled by *{1}* from *{2}.{3}* at IP address *{4}* on *{5}*.**

Explanation

Substitution variables are:

*{0}*Operation name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Network ID
*{5}*IP address

745 **The following operation completed successfully: *{0}*. It was scheduled by *{1}* from *{2}.{3}* on *{4}*.**

Explanation

Substitution variables are:

*{0}*Operation name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Network ID

746 **The following operation completed successfully: *{0}*. It was scheduled by *{1}* from *{2}.{3}* at IP address *{4}* on *{5}*.**

Explanation

Substitution variables are:

*{0}*Operation name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Network ID
*{5}*IP address

747 **The RSF queue has been put on hold.**

748 **The RSF queue has been released from hold.**

749 **The *{0}* object was defined.**

Explanation

Substitution variables are:

*{0}*Object name

750 **The *{0}* object was undefined.**

Explanation

Substitution variables are:

*{0}*Object name

751 **Upgrade data was saved.**

752 **The CBU file was deleted from the hard disk.**

753 **An error was detected trying to delete the CBU file.**

754	**PMI Upgrade was successful.**
755	**PMI Upgrade failed or was not required.**
756	**User *{0}* logged off from a Platform Independent Remote Console (PIRC) at IP address *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*IP address

757	**User *{0}* was logged off from a Platform Independent Remote Console (PIRC) at IP address *{1}* due to inactivity.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*IP address

776	**Mirroring data from the primary Support Element to the alternate Support Element completed successfully.**
777	**A switch request initiated the alternate Support Element (serial number *{0}*) to now be the primary Support Element.**

Explanation

Substitution variables are:

*{0}*Serial number

778	**Mirroring data from the primary Support Element to the alternate Support Element started.**
779	**Mirroring data from the primary Support Element to the alternate Support Element failed. *{0}***

Explanation

Substitution variables are:

*{0}*Reason for the failure

780	**An alternate Support Element is not installed. Mirroring data from the primary Support Element could not be completed.**
781	**The following operation completed: *{0}*. It was scheduled by *{1}* from *{2}* on *{3}*.**

Explanation

Substitution variables are:

*{0}*Description of operation
*{1}*User name
*{2}*Console name
*{3}*Date

782	**The following operation completed: *{0}*. It was scheduled by *{1}* from *{2}*.*{3}* at IP address *{4}* on *{5}*.**

Explanation

Substitution variables are:

*{0}*Description of operation
*{1}*User name
*{2}*Network ID
*{3}*NAU
*{4}*IP address
*{5}*NAU

783	**The CBU feature has been enabled successfully.**
784	**An error was detected trying to enable the CBU feature.**
785	**A concurrent CP upgrade was performed to add *{0}* CPUs.**

Explanation

Substitution variables are:

*{0}*Number of CPs

786	**A special code load was performed.**
787	**Domain security name or password was changed on consoles: *{0}*.**

Explanation

Substitution variables are:

*{0}*Console names

788	**Remote request made to change the Support Element name.**
789	**Remote request made to reboot the Support Element.**
790	**Alternate Support Element rebooted upon completing a mirroring operation.**
791	**Switched from primary to alternate Support Element.**
792	**Switched from primary to alternate Support Element after LAN recovery.**
793	**Support Element rebooted to apply patches during concurrent patch.**
794	**Support Element rebooted to apply patches during disruptive patch.**
795	**Local request made to change the Support Element name.**
797	**Due to event log space limitations, obsolete events were deleted and file *{0}* was created.**

Explanation

Substitution variables are:

*{0}*Log file name

798	**The number of CPs for partition *{0}* has changed from *{1}* to *{2}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Old number of CPs
*{2}*New number of CPs

799 **The global IO priority queuing setting has been *{0}*.**

Explanation

Substitution variables are:

*{0}*Enabled or disabled

800 **Settings for logical partitions IO priority queuing were changed.**

Messages 801-900

801 **The current processing capped value for partition *{0}* changed from *{1}* to *{2}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Old processing capped value
*{2}*New processing capped value

802 **The current processing weight value for partition *{0}* changed from *{1}* to *{2}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Old processing weight value
*{2}*New processing weight value

803 **A *{0}* Alternate Support Element switch is requested by *{1}* from *{2}.{3}*.**

Explanation

Substitution variables are:

*{0}*Switch type
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU

804 **A *{0}* Alternate Support Element switch is requested by *{1}* from *{2}.{3}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Switch type
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Origin IP address

805 **A *{0}* Alternate Support Element switch was initiated from *{1}*.**

Explanation

Substitution variables are:

*{0}*Switch type
*{1}*Console requesting switch

806	**An automatic alternate Support Element switch was initiated due to *{0}*.**

Explanation

Substitution variables are:

*{0}*Reason for the switch

807	**A *{0}* Alternate Support Element switch is requested for *{1}.{2}* by *{3}* from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Switch type
*{1}*Network ID
*{2}*NAU
*{3}*HMC user name
*{4}*Origin Network ID
*{5}*Origin NAU

808	**Channel upgrade completed successfully.**
809	**Channel upgrade failed.**
810	**Channel upgrade was partially successful.**
811	**The import of the PCI cryptographic coprocessor FCV file was successful.**
812	**The zeroize of the PCI cryptographic coprocessor *{0}* was successful.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

813	**The zeroize of the PCI cryptographic coprocessor configuration was successful.**
814	**Electronic Service Agent I/O Service data transfer completed.**
815	**Electronic Service Agent I/O Service data transfer failed.**
816	**Electronic Service Agent Software Service data transfer completed.**
817	**Electronic Service Agent Software Service data transfer failed.**
818	**Electronic Service Agent Registration completed.**
819	**Electronic Service Agent Registration failed.**
820	**System configuration file bbruchpd.dat was deleted.**
821	**CHPID mapping function completed.**
822	**Linux CP feature update completed.**
823	**Linux CP feature update failed.**
824	**UNDO Linux CP feature completed.**
825	**UNDO Linux CP feature update failed.**
826	**Remote support call generated on *{1}* failed at server *{0}*. Reason: Machine is not under warranty or service contract.**

Explanation

Substitution variables are:

*{0}*Destination machine name and IP address
*{1}*Origin machine name

827 **A concurrent CP downgrade was performed. Current number of *{1}* are *{0}*.**

Explanation

Substitution variables are:

*{0}*Type of CP
*{1}*Number of CPs

828 **A concurrent memory upgrade was performed to add *{0}* MBytes.**

Explanation

Substitution variables are:

*{0}*Number of MBytes

829 **A concurrent memory downgrade was performed to remove *{0}* MBytes.**

Explanation

Substitution variables are:

*{0}*Number of MBytes

830 **An import of the PCI cryptographic coprocessor UDX image was successful.**

831 **The activation of the UDX image for PCI cryptographic coprocessor *{0}* was successful. Timestamp: *{1}*, Name: *{2}***

Explanation

Substitution variables are:

*{0}*Cryptographic number
*{1}*Timestamp
*{2}*Segment 3 image name

832 **The activation of the factory default image for PCI cryptographic coprocessor *{0}* was successful.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

833 **The zeroize of the PCI cryptographic coprocessor UDX image was successful.**

834 **Unable to inform the operating system about the model conversion.**

835 **PU LICCC record has been retrieved from support system.**

836 **CBU LICCC record has been retrieved from support system.**

837 **MEM LICCC record has been retrieved from support system.**

838 **CHN LICCC record has been retrieved from support system.**

839 **DRA record has been retrieved from support system.**

840	**LCP record has been retrieved from support system.**
841	**PU LICCC record has been deleted from the hard disk.**
842	**CBU LICCC record has been deleted from the hard disk.**
843	**MEM LICCC record has been deleted from the hard disk.**
844	**CHN LICCC record has been deleted from the hard disk.**
845	**DRA record has been deleted from the hard disk.**
846	**LCP record has been deleted from the hard disk.**
847	**Concurrent internal code changes for oFCP loader started.**
848	**Concurrent internal code changes for oFCP loader completed.**
849	**Concurrent internal code changes for oFCP loader failed.**
850	**Mirroring over the customer network, because the service network is down.**
851	**CIU LICCC record has been retrieved from support system.**
852	**CIU LICCC record has been deleted from the hard disk.**
853	**Input/Output Configuration Data Sets (IOCDS) restored from *{0}* *{1}*.**

Explanation

Substitution variables are:

*{0}*HMC Network ID
*{1}*HMC NAU

854	**Processor drawer hardware was added at *{0}*.**

Explanation

Substitution variables are:

*{0}*Location for the processor drawer

855	**Processor drawer hardware was deleted from *{0}*.**

Explanation

Substitution variables are:

*{0}*Location for the processor drawer

856	**Concurrent processor drawer hardware add completed successfully.**
857	**Concurrent processor drawer hardware add failed.**
858	**System Complex (Sysplex) Timer was used to change ETR configuration data.**
859	**There have been *{0}* consecutive failed logon attempts for user *{1}*.**

Explanation

Substitution variables are:

*{0}*Number of failed logon attempts
*{1}*User name

860	**Backup critical console data failed, *{0}*.**

Explanation

Substitution variables are:

*{0}*State of the backup

861	**Backup critical console data completed.**
862	**Permanent LICCC update completed successfully.**
863	**Permanent LICCC update failed.**
864	**Root password was updated.**
865	**An Authorize internal code changes request of *{0}* for Hardware Management Console *{1}.{2}* and all its defined objects is being issued by *{3}* from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Request type
*{1}*HMC Network ID
*{2}*HMC NAU
*{3}*User name
*{4}*HMC Network ID
*{5}*HMC NAU

866	**The CP cryptographic assist functions have been enabled successfully.**
867	**The CP cryptographic assist functions have been disabled successfully.**
868	**System power on started for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

869	**System power on completed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

870	**System power on failed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

871	**System restricted power on started for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

872	**System restricted power on completed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

873 **System restricted power on failed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

874 **System power off started for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

875 **System power off completed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

876 **System power off failed for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

877 **An EC upgrade has been performed on this Support Element.**

878 **A preload has been performed on this alternate Support Element.**

879 **The scheduled *{0}* did not run because the system was running and force was not specified. It was scheduled by *{1}* from *{2}.{3}* on *{4}*.**

Explanation

Substitution variables are:

*{0}*Operation name
*{1}*User name
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Timestamp

881 **The TKE commands for PCIX cryptographic coprocessor number *{0}* have been enabled successfully.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

882 **The TKE commands for PCIX cryptographic coprocessor number *{0}* have been disabled successfully.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

883 **Refresh request for customizing console data via the LAN from *{0}*@*{1}* was ignored since this capability is disabled.**

Explanation

Substitution variables are:

*{0}*Host name
*{1}*IP address

884 **A request to customize console data via the LAN from *{0}*@*{1}* was ignored since this capability is disabled.**

Explanation

Substitution variables are:

*{0}*Host name
*{1}*IP address

885 **Customizable console data (*{2}*) has been sent via the LAN to *{0}*@*{1}*.**

Explanation

Substitution variables are:

*{0}*Host name
*{1}*IP address
*{2}*Customizable console data type

886 **Customizable console data (*{2}*) has been received via the LAN from *{0}*@*{1}*.**

Explanation

Substitution variables are:

*{0}*Host name
*{1}*IP address
*{2}*Customizable console data type

887 **The following disruptive operation started: Deactivate. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

888 **The following disruptive operation started: Deactivate. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

---

889 **The following disruptive operation started: Disable concurrent patch. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

---

890 **The following disruptive operation started: Disable concurrent patch. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

---

891 **The following disruptive operation started: Install code changes/Activate. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

---

892 **The following disruptive operation started: Install code changes/Activate. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

---

893 **The following disruptive operation started: Load. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type

*{1}*Origin Network ID
*{2}*Origin NAU

894 **The following disruptive operation started: Load. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

895 **The following disruptive operation started: Power off. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

896 **The following disruptive operation started: Power off. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

897 **The following disruptive operation started: Power-on reset. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

898 **The following disruptive operation started: Power-on reset. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

899 **The following disruptive operation started: PSW restart. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

900 **The following disruptive operation started: PSW restart. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

Messages 901-1000

901 **The following disruptive operation started: Remove code changes/activate. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

902 **The following disruptive operation started: Remove code changes/activate. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

903 **The following disruptive operation started: Reset I/O interface. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

904 **The following disruptive operation started: Reset I/O interface. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

905 **The following disruptive operation started: Run checkout tests. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

906 **The following disruptive operation started: Run checkout tests. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

907 **The following disruptive operation started: Set clock. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

908 **The following disruptive operation started: Set clock. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

909 **The following disruptive operation started: Stop. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type

*{1}*Origin Network ID
*{2}*Origin NAU

910 **The following disruptive operation started: Stop. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

911 **The following disruptive operation started: Sysplex timer configuration change. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

912 **The following disruptive operation started: Sysplex timer configuration change. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

913 **The following disruptive operation started: System reset. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

914 **The following disruptive operation started: System reset. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

915 **The following disruptive operation started: System reset normal for object *{0}*. It was requested by *{1}* from *{2}.{3}*.**

Explanation

Substitution variables are:

*{0}*Target object name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU

916 **The following disruptive operation started: System reset normal for object *{0}*. It was requested by *{1}* from *{2}.{3}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Target object name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Origin IP address

917 **The following disruptive operation started: System reset clear for object *{0}*. It was requested by *{1}* from *{2}.{3}*.**

Explanation

Substitution variables are:

*{0}*Target object name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU

918 **The following disruptive operation started: System reset clear for object *{0}*. It was requested by *{1}* from *{2}.{3}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Target object name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Origin IP address

919 **The following disruptive operation started: Unknown. It was requested by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

920 **The following disruptive operation started: Unknown. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

921 **A load will be attempted for system *{0}*. The load type is normal, store status yes, address *{2}*, parameter *{1}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Load address
*{2}*Load parameter

922 **A load will be attempted for system *{0}*. The load type is normal, store status no, address *{2}*, parameter *{1}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Load address
*{2}*Load parameter

923 **A load will be attempted for system *{0}*. The load type is clear, store status yes, address *{2}*, parameter *{1}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Load address
*{2}*Load parameter

924 **A load will be attempted for system *{0}*. The load type is clear, store status no, address *{2}*, parameter *{1}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Load address
*{2}*Load parameter

925 **A load will be attempted for system *{0}*. The load type is SCSI. Refer to the security log for more details.**

Explanation

Substitution variables are:

*{0}*Image name

---

926 **A load will be attempted for system *{0}*. The load type is SCSI dump. Refer to the security log for more details.**

Explanation

Substitution variables are:

*{0}*Image name

---

927 **A load will be attempted for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Image Name

---

928 **The following disruptive operation started: Activate. It was requested by *{0}* from *{1}*. *{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

---

929 **The following disruptive operation started: Activate. It was requested by *{0}* from *{1}*. *{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

---

930 **The following disruptive operation started: Configure channel off. It was requested by *{0}* from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

---

931 **The following disruptive operation started: Configure channel off. It was requested by *{0}* from *{1}*.*{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

932 **Activation has started using the reset profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name

933 **Activation has started using the image profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Image profile name

934 **Activation has started using the load profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Load profile name

935 **Automatic activation has started using the reset profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name

936 **Automatic activation has started using the image profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Image profile name

937 **Automatic activation has started using the load profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Load profile name

938 **User *{0}* with session ID *{1}* has requested to *{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Logon session identifier
*{2}*Type of shutdown

939 **An LPAR dump, initiated by a B3 PCCALL, has been taken.**

940 **An LPAR dump, initiated by the LPAR Dump Task, has been taken.**

941 **An LPAR dump, initiated by a disabled wait, has been taken.**

942 **The global IO Priority Queuing setting is *{0}* (0=disabled, 1=enabled).**

Explanation

Substitution variables are:

*{0}*1 if enabled, 0 if disabled

943 **The current processing capped value for the *{1}* CPs in partition *{0}* changed from *{2}* to *{3}* (0=not capped, 1=capped).**

Explanation

Substitution variables are:

*{0}*Type of CPs
*{1}*Image name
*{2}*Old processing capped value
*{3}*New processing capped value

944 **The *{0}* object was locked from disruptive tasks by *{1}*.**

Explanation

Substitution variables are:

*{0}*Object name
*{1}*User name

945 **The *{0}* object was unlocked from disruptive tasks by *{1}*.**

Explanation

Substitution variables are:

*{0}*Object name
*{1}*User name

947 **A concurrent resource change has resulted in a change to the processor speed.**

948 **A user password was changed.**

949 **Channel confg files swap completed for channels *{0}* and *{1}*.**

Explanation

Substitution variables are:

*{0}*PCHID name
*{1}*PCHID name

950 **Dynamic partition rename was used to *{0}* logical partition *{1}*. The partition number is *{2}*, CSS ID is *{3}*, image ID is *{4}*.**

Explanation

Substitution variables are:

*{0}*add or remove
*{1}*Image name

*{2}*Partition number
*{3}*CSS identifier
*{4}*Image identifier

951 **Change CP/SAP allocation has started.**

952 **Change CP/SAP allocation has completed successfully.**

953 **Change CP/SAP allocation has failed.**

954 **A concurrent CP upgrade was performed to add *{0} {1}*.**

Explanation

Substitution variables are:

*{0}*Number of CPs
*{1}*Type of CP

955 **A concurrent resource change has resulted in a change to the processor speed.**

956 **The reset profile *{0}* was created.**

Explanation

Substitution variables are:

*{0}*Profile name

957 **The load profile *{0}* was created.**

Explanation

Substitution variables are:

*{0}*Profile name

958 **The image profile *{0}* was created.**

Explanation

Substitution variables are:

*{0}*Profile name

959 **The system activity profile *{0}* was created.**

Explanation

Substitution variables are:

*{0}*Profile name

960 **The reset profile *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*Profile name

961 **The load profile *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*Profile name

962 **The image profile *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*Profile name

963 **The system activity profile *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*Profile name

964 **The reset profile *{0}* was upgraded.**

Explanation

Substitution variables are:

*{0}*Profile name

965 **The load profile *{0}* was upgraded.**

Explanation

Substitution variables are:

*{0}*Profile name

966 **The image profile *{0}* was upgraded.**

Explanation

Substitution variables are:

*{0}*Profile name

967 **The system activity profile *{0}* was upgraded.**

Explanation

Substitution variables are:

*{0}*Profile name

968 **The reset profile *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*Profile name

969 **The load profile *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*Profile name

970 **The image profile *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*Profile name

971 **The system activity profile *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*Profile name

972 **The reset profile *{0}* was imported.**

Explanation

Substitution variables are:

*{0}*Profile name

973 **The load profile *{0}* was imported.**

Explanation

Substitution variables are:

*{0}*Profile name

974 **The image profile *{0}* was imported.**

Explanation

Substitution variables are:

*{0}*Profile name

975 **The system activity profile *{0}* was imported.**

Explanation

Substitution variables are:

*{0}*Profile name

976 **Load from removable media or server for image *{0}* completed successfully.**

Explanation

Substitution variables are:

*{0}*Image name

977 **Load from removable media or server for image *{0}* failed.**

Explanation

Substitution variables are:

*{0}*Image name

978 **Load from removable media or server for image *{0}* failed. Not enough memory in the image available.**

Explanation

Substitution variables are:

*{0}*Image name

979 **Load from removable media or server for image *{0}* has failed. There was a problem trying to read all of the data files.**

Explanation

Substitution variables are:

*{0}*Image name

980 **Dumping of SCSI IPL loader data for image *{0}* completed successfully.**

Explanation

Substitution variables are:

*{0}*Image name

981 **Dumping of SCSI IPL loader data for image *{0}* failed.**

Explanation

Substitution variables are:

*{0}*Image name

982 **The following operation started: Concurrent switch. It was requested by *{0}* from *{1}*. *{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

983 **The following operation started: Concurrent switch. It was requested by *{0}* from *{1}*. *{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

984 **The following operation started: Disruptive switch. It was requested by *{0}* from *{1}*. *{2}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

985 **The following operation started: Disruptive switch. It was requested by *{0}* from *{1}*. *{2}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address

986 **Channel upgrade started.**

987 **Rebuild VPD started.**

988 **CBU activation started.**

989 **CIU retrieve started.**

990 **Apply retrieved data started.**

991 **OOCOD activation started.**

992 **CBU/OOCOD undo started.**

993 **A change of system performance values has started that will *{0}*.**

Explanation

Substitution variables are:

*{0}*Description of the change

994 **A change of system performance values has completed successfully.**

995 **A change of system performance values has failed.**

996 **Rebuild VPD failed.**

997 **Rebuild of VPD is only partially complete.**

998 **CIU retrieve failed.**

999 **Maximum available memory feature added OK**

1000 **Error adding the maximum available Memory feature**

Messages 1001-1100

1001 **Maximum available memory feature was removed OK**

1002 **Error removing the mMaximum available memory feature**

1003 **Start add STP feature.**

1004 **Add STP feature failed.**

1005	**Add STP feature was successful.**
1006	**Start add FSB feature.**
1007	**Add FSB feature failed**
1008	**Add FSB feature was successful.**
1009	**Start remove STP feature.**
1010	**Remove STP feature failed.**
1011	**Remove STP feature was successful.**
1012	**Start remove FSB feature.**
1013	**Remove FSB feature failed**
1014	**Remove FSB feature was successful.**
1015	**Restore critical data was started.**
1016	**Start add RPQ 8P2333 feature.**
1017	**Add RPQ 8P2333 feature failed.**
1018	**Add RPQ 8P2333 feature was successful.**
1019	**Start remove RPQ 8P2333 feature.**
1020	**Remove RPQ 8P2333 feature failed.**
1021	**Remove RPQ 8P2333 feature was successful.**
1022	**Add RPQ 8P2333 feature was partially successful.**
1023	**Transmit VPD task entering sleep.**
1024	**Transmit VPD task waking.**
1025	**Start add OSA 3215 feature.**
1026	**Add OSA 3215 feature failed.**
1027	**Add OSA 3215 feature was successful.**
1028	**Start remove OSA 3215 feature.**
1029	**Remove OSA 3215 feature failed.**
1030	**Remove OSA 3215 feature was successful.**
1031	**Add OSA 3215 feature was partially successful.**
1044	**Start add of three phase power cord feature.**
1045	**Add three phase power cord feature failed.**
1046	**Add three phase power cord feature was successful.**
1047	**Start remove of three phase power cord feature.**
1048	**Remove three phase power cord feature failed.**
1049	**Remove three phase power cord feature was successful.**
1050	**Start add of alternate CP assignment feature.**
1051	**Add alternate CP assignment feature failed.**
1052	**Add alternate CP assignment feature was successful.**
1053	**Start remove of alternate CP assignment feature.**
1054	**Remove alternate CP assignment feature failed.**

1055 **Remove alternate CP Assignment feature was successful.**

1056 **Start synchronization with HOM.**

1057 **Start add of *{0}* feature.**

Explanation

Substitution variables are:

*{0}*Feature name

1058 **Add of *{0}* feature failed.**

Explanation

Substitution variables are:

*{0}*Feature name

1059 **Add of *{0}* feature was successful.**

Explanation

Substitution variables are:

*{0}*Feature name

1060 **Start remove of *{0}* feature.**

Explanation

Substitution variables are:

*{0}*Feature name

1061 **Remove of *{0}* feature failed.**

Explanation

Substitution variables are:

*{0}*Feature name

1062 **Remove of *{0}* feature was successful.**

Explanation

Substitution variables are:

*{0}*Feature name

1063 **The *{0}* object was set to busy by *{1}*.**

Explanation

Substitution variables are:

*{0}*Target name
*{1}*User name

1064 **The *{0}* object was set to not busy by *{1}*.**

Explanation

Substitution variables are:

*{0}*Target name
*{1}*User name

1065	**Unexpected error.**
1066	**Record *{0}* contains System z Application Assist Processors (zAAPs) and has been deleted.**

Explanation

Substitution variables are:

*{0}*Record number

1067	**Domain security name or password was changed by console *{0}*.**

Explanation

Substitution variables are:

*{0}*Console name

1068	**Backup critical data completed successfully.**
1069	**Backup critical data was attempted but was not successful.**
1070	**Backup critical data encountered an error when creating the backup.**
1071	**Backup critical data completed successfully, but it was not sent to the FTP server.**
1100	**The system clock has changed.**

Messages 1101-1200

1101	**The leap second offset has changed to *{0}* seconds.**

Explanation

Substitution variables are:

*{0}*Seconds

1102	**The time zone parameters have changed.**
1103	**The coordinated timing network ID for this CPC has changed to *{0}*.**

Explanation

Substitution variables are:

*{0}*Coordinated timing network identifier

1104	**The network configuration for the coordinated timing network that this CPC is a member of has changed.**
1105	**This CPC is configured as a local clock server for the coordinated timing network that it is a member of.**
1106	**This CPC is no longer configured as a local clock server for the coordinated timing network that it is a member of.**
1107	**This CPC changed the coordinated timing network ID for the coordinated timing network to *{0}* as requested.**

Explanation

Substitution variables are:

*{0}*Coordinated timing network identifier

1108	**This CPC changed the network configuration for the coordinated timing network as requested.**
1109	**This CPC changed the network configuration for the coordinated timing network because of a recovery action.**
1110	**This CPC is requesting an adjustment to the coordinated server time after contacting an external time source via *{0}*.**

Explanation

Substitution variables are:

*{0}*External time source type and the amount of time to adjust

1111	**The migration procedure from an STP-only Coordinated Timing Network (CTN) to a mixed CTN started.**
1112	**The migration procedure from an STP-only Coordinated Timing Network (CTN) to a mixed CTN completed successfully.**
1113	**The migration procedure from an STP-only Coordinated Timing Network (CTN) to a mixed CTN was cancelled.**
1114	**The migration procedure from an STP-only Coordinated Timing Network (CTN) to a mixed CTN failed.**
1115	**Automatic adjustment of the coordinated server time to an external time source failed because the threshold was exceeded.**
1116	**Automatic adjustment of the coordinated server time to an external time source failed.**
1117	**A timeout occurred contacting the external time source to automatically adjust the coordinated server time.**
1118	**Detected another STP-only Coordinated Timing Network (CTN) with the same CTN ID.**
1119	**Lost clock synchronization.**
1120	**Pulse Per Second (PPS) signals are being used to provide highly accurate adjustments to the coordinated server time for the STP-only CTN.**
1121	**Pulse Per Second (PPS) signals are no longer being used to provide highly accurate adjustments to the coordinated server time for the STP-only CTN, as requested by the user.**
1122	**Automatic adjustment of the coordinated server time to an external time source failed because no Hardware Management Console is set up to perform the dial out.**
1123	**PPS port 0 *{0}* receiving Pulse Per Second (PPS) signals.**

Explanation

Substitution variables are:

*{0}*is or is not

1124	**PPS port 1 *{0}* receiving Pulse Per Second (PPS) signals.**

Explanation

Substitution variables are:

*{0}*is or is not

1125 **PPS port *{0}* is no longer synchronized.**

Explanation

Substitution variables are:

*{0}*Port number

1126 **PPS port *{0}* offset differs by more than the amount allowed from the PPS port that is tracking to PPS signal.**

Explanation

Substitution variables are:

*{0}*Port number

1127 **A configuration error was detected on PPS port *{0}*.**

Explanation

Substitution variables are:

*{0}*Port number

1128 **PPS port *{0}* dispersion is greater than the threshold value.**

Explanation

Substitution variables are:

*{0}*Port number

1129 **A jam synch condition was detected on PPS port *{0}*.**

Explanation

Substitution variables are:

*{0}*Port number

1130 **Pulse Per Second (PPS) signals from PPS port 0 are being used.**

1131 **Pulse Per Second (PPS) signals from PPS port 1 are being used.**

1132 **Receiving Pulse Per Second (PPS) signals on port *{0}* to provide redundancy of an External Time Source.**

Explanation

Substitution variables are:

*{0}*Port number

1133 **No longer receiving Pulse Per Second (PPS) signals.**

1134 **Adjustments to coordinated server time for the STP-only CTN are being made using information from the backup system.**

1135 **Adjustments to coordinated server time for the STP-only CTN are no longer being made using information from the backup system.**

1136 **PPS port *{0}* offset on the backup system differs by more than the amount allowed from the PPS port that is tracking to PPS signal.**

Explanation

Substitution variables are:

*{0}*Port number

1137	**Pulse Per Second (PPS) signals are no longer being used to provide highly accurate adjustments to the Coordinated Server Time for the STP-only CTN due to a failure.**
1138	**Daylight saving time started.**
1139	**Daylight saving time ended.**
1140	**The STP maximum supported version number or lowest supported version number for this CPC changed to version *{0}*.**

Explanation

Substitution variables are:

*{0}*Version number

1141	**The total time offset changed.**
1142	**The network configuration for your STP-only CTN cannot be reestablished after a power-on reset or power outage.**
1143	**Pulse Per Second (PPS) port 0 *{0}* usable as a PPS source.**

Explanation

Substitution variables are:

*{0}*is or is not

1144	**Pulse Per Second (PPS) port 1 *{0}* usable as a PPS source.**

Explanation

Substitution variables are:

*{0}*is or is not

1145	**Pulse Per Second (PPS) port *{0}* entered a fenced state.**

Explanation

Substitution variables are:

*{0}*Port number

1146	**Automated coordinated timing network recovery is enabled on this CPC.**
1147	**Automated coordinated timing network recovery is disabled on this CPC: *{0}*.**

Explanation

Substitution variables are:

*{0}*The reason the automated coordinated timing network recovery is disabled.

1148	**The joining of STP CTN *{0}* into another CTN has started.**

Explanation

Substitution variables are:

*{0}*Coordinated timing network identifier

1149 **The joining of STP CTN *{0}* into another CTN has been cancelled.**

Explanation

Substitution variables are:

*{0}*Coordinated timing network identifier

1150 **The joining of two STP CTNs into one has failed: *{0}*.**

Explanation

Substitution variables are:

*{0}*The reason the join of two CTNs failed.

1200 **Customizable console data (*{0}*) was resynchronized by user *{1}*.**

Explanation

Substitution variables are:

*{0}*Customizable data name
*{1}*User name

Messages 1201-1300

1201 **Customizable console data (*{0}*) was deconfigured from all sources by user *{1}*.**

Explanation

Substitution variables are:

*{0}*Customizable data name
*{1}*User name

1202 **Customizable console data (*{0}*) was changed manually by user *{1}*.**

Explanation

Substitution variables are:

*{0}*Customizable data name
*{1}*User name

1203 **The managed objects role *{0}* has been created.**

Explanation

Substitution variables are:

*{0}*User role name

1204 **The managed objects role *{0}* has been changed.**

Explanation

Substitution variables are:

*{0}*User role name

1205 **The managed objects role *{0}* has been deleted.**

Explanation

Substitution variables are:

*{0}*User role name

1206	**Enable CBU feature started.**
1207	**CBU UNDO failure.**
1208	**CBU UNDO was partially successful.**
1209	**Start delete CBU feature.**
1210	**CBU feature activation was successful.**
1211	**CBU feature activation failed.**
1212	**CBU feature activation was partially successful.**
1213	**OOCoD UNDO was successful.**
1214	**OOCoD UNDO failed.**
1215	**OOCoD UNDO was partially successful.**
1216	**OOCoD feature activation was successful.**
1217	**OOCoD feature activation was partially successful.**
1218	**OOCoD feature activation failed.**
1219	**The zeroize of the cryptographic number *{0}* was successful.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

1220	**The zeroize of the cryptographic configuration was successful.**
1221	**The cryptographic UDX image *{0}* was successfully imported from media.**

Explanation

Substitution variables are:

*{0}*UDX image name

1222	**The activation of the UDX image for cryptographic coprocessor *{0}* was successful. Timestamp: *{1}*, Name: *{2}***

Explanation

Substitution variables are:

*{0}*Cryptographic number
*{1}*Timestamp
*{2}*UDX image name

1223	**The activation of the factory default image for cryptographic coprocessor *{0}* was successful.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

1224 **The erase of the cryptographic coprocessor UDX image *{0}* was successful.**

Explanation

Substitution variables are:

*{0}*UDX image name

1225 **The TKE commands for cryptographic coprocessor number *{0}* have been enabled successfully.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

1226 **The TKE commands for cryptographic coprocessor number *{0}* have been disabled successfully.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

1227 **OOCoD remove failed.**

1228 **CBU remove failed.**

1229 **CIU apply failed.**

1230 **CIU apply was successful.**

1231 **Undo temporary upgrade started.**

1232 **Undo CBU was successful.**

1233 **The configuration type of cryptographic number *{0}* has been changed to cryptographic accelerator.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

1234 **The configuration type of cryptographic number *{0}* has been changed to a cryptographic CCA coprocessor.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

1235 **Concurrent upgrade Engineering Changes (EC) activate of system EC *{0}* started by *{1}* from *{2}.{3}*.**

Explanation

Substitution variables are:

*{0}*System EC number
*{1}*User name
*{2}*Originating Network ID

*{3}*Originating NAU

1236 **Concurrent upgrade Engineering Changes (EC) activate of system EC *{0}* completed.**

Explanation

Substitution variables are:

*{0}*System EC number

1237 **Concurrent upgrade Engineering Changes (EC) activate of system EC *{0}* failed.**

Explanation

Substitution variables are:

*{0}*System EC number

1238 **Prepare for concurrent processor drawer replacement started.**

1239 **PU check for concurrent processor drawer replacement started.**

1240 **PUS are prepared for concurrent processor drawer replacement.**

1241 **PUS are not ready for concurrent processor drawer replacement.**

1242 **Prepare for concurrent processor drawer replacement failed during PU check.**

1243 **Memory check for concurrent processor drawer replacement started.**

1244 **Memory is prepared for concurrent processor drawer replacement.**

1245 **Memory is not ready for concurrent processor drawer replacement.**

1246 **Prepare for concurrent processor drawer replacement failed during memory check.**

1247 **I/O check for concurrent processor drawer replacement started.**

1248 **I/O is prepared for concurrent processor drawer replacement.**

1249 **I/O is not ready for concurrent processor drawer replacement.**

1250 **Prepare for concurrent processor drawer replacement failed during I/O check.**

1251 **Prepare for concurrent processor drawer replacement was successful.**

1252 **System is not ready for concurrent processor drawer replacement.**

1253 **Prepare for concurrent processor drawer replacement failed.**

1254 **Perform concurrent processor drawer replacement started.**

1255 **Perform concurrent processor drawer replacement was successful.**

1256 **Perform concurrent processor drawer replacement failed.**

1257 **Upgrade data restore was successful. Restore type is *{0}*.**

Explanation

Substitution variables are:

*{0}*Type of restore data

1258 **Upgrade data restore was unsuccessful. Restore type is *{0}*.**

Explanation

Substitution variables are:

*{0}*Type of restore data

1259	**Concurrent processor drawer hardware add started.**
1260	**Concurrent processor drawer hardware add LICCC data error.**
1261	**Book LICCC upgrade started.**
1262	**Concurrent upgrade Engineering Changes (EC) activate of system EC *{0}* for *{1}.{2}* started by *{3}* from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*System EC number
*{1}*Destination Network ID
*{2}*Destination NAU
*{3}*User name
*{4}*Originating Network ID
*{5}*Originating NAU

1263	**Concurrent internal code changes initiated by concurrent upgrade engineering changes activate request.**
1264	**Add processor drawer hardware request was cancelled.**
1265	**Concurrent upgrade Engineering Changes (EC) activate of system EC *{0}* completed, but not all functions may be available until the next system activation.**

Explanation

Substitution variables are:

*{0}*System EC number

1266	**BFYCALL request included: *{0}* CPS, *{1}* SAPS, *{2}* ICFS, *{3}* IFLS, *{4}* zIIPS, *{5}* IFPs.**

Explanation

Substitution variables are:

*{0}*Number of CPs
*{1}*Number of SAPs
*{2}*Number of ICFs
*{3}*Number of IFLs
*{4}*Number of zIIPs
*{5}*Number of IFPs

1267	**NULL user ID found.**
1268	**Remote support call generated on *{1}* failed at server *{0}*. Reason: No call home server is available.**

Explanation

Substitution variables are:

*{0}*IP address of the machine handling the request
*{1}*Originating machine name

1269	**An attempt was made to accept internal code changes but there were none to accept.**

1270 **The Monitor System Events task sent an email to *{0}* with a message count of *{1}* for sources *{2}*.**

Explanation

Substitution variables are:

*{0}*Destination name
*{1}*Number of messages
*{2}*Source name

1271 **Remote request made to reboot the console by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Network ID
*{2}*NAU

1272 **The task role *{0}* has been created.**

Explanation

Substitution variables are:

*{0}*Task role name

1273 **The task role *{0}* has been changed.**

Explanation

Substitution variables are:

*{0}*Task role name

1274 **The task role *{0}* has been deleted.**

Explanation

Substitution variables are:

*{0}*Task role name

1275 **The current processing weight value for the *{0}* CPs in partition *{1}* changed from *{2}* to *{3}*.**

Explanation

Substitution variables are:

*{0}*Type of CPs
*{1}*Image name
*{2}*Old weight value
*{3}*New weight value

1276 **A SOO session to the remote system was started for remote system user *{0}* from *{1}* for Hardware Management Console user *{2}*.**

Explanation

Substitution variables are:

*{0}*SE user name
*{1}*HMC name
*{2}*HMC user name

1277 **A SOO session to the remote system was ended for remote system user *{0}* from *{1}*.**

Explanation

Substitution variables are:

*{0}*SE user name
*{1}*HMC name

1278 **The password for user *{0}* has changed.**

Explanation

Substitution variables are:

*{0}*User name

1279 **User *{0}* has logged on.**

Explanation

Substitution variables are:

*{0}*User name

1280 **User *{0}* has logged off.**

Explanation

Substitution variables are:

*{0}*User name

1281 ***{0}***

Explanation

Substitution variables are:

*{0}*User name

1282 ***{0}***

Explanation

Substitution variables are:

*{0}*User name

1283 ***{0}* was forcibly disconnected by Hardware Management Console user *{2}* on *{1}*.**

Explanation

Substitution variables are:

*{0}*Current SE user information
*{1}*New HMC name

*{2}*New HMC user name

1284 **User *{0}* of session *{1}* has forcibly disconnected user *{2}* of session *{3}* in order to log on locally.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Logon session identifier
*{2}*Disconnected user name or '?' if unknown
*{3}*Disconnected session identifier

1285 **User *{0}* was not permitted to log on or reconnect since another user is already logged on.**

Explanation

Substitution variables are:

*{0}*User name

1286 **User *{0}* was not permitted to log on since the userid is disabled.**

Explanation

Substitution variables are:

*{0}*User name

1287 **User *{0}* was not permitted to log on since the userid is not allowed remote access.**

Explanation

Substitution variables are:

*{0}*User name

1288 **Remote request made to restart the console by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Network ID
*{2}*NAU

1289 **Remote request made to power off the console by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Network ID
*{2}*NAU

1290 **Remote request made to shutdown the console by *{0}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Network ID
*{2}*NAU

1292 **The user profile *{0}* was created.**

Explanation

Substitution variables are:

*{0}*User profile name

1293 **The user profile *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*User profile name

1294 **The managed objects role *{0}* has been created.**

Explanation

Substitution variables are:

*{0}*Managed object role name

1295 **The managed objects role *{0}* has been changed.**

Explanation

Substitution variables are:

*{0}*Managed object role name

1296 **The task role *{0}* has been created.**

Explanation

Substitution variables are:

*{0}*Task role name

1297 **The task role *{0}* has been changed.**

Explanation

Substitution variables are:

*{0}*Task role name

1298 **Media device "*{0}*" lock held by "*{1}*" has been unlocked.**

Explanation

Substitution variables are:

*{0}*Media device name
*{1}*Lock owner

1299 **Media device "*{0}*" lock held by "*{1}*" failed to unlock.**

Explanation

Substitution variables are:

*{0}*Media device name
*{1}*Lock owner

1300 **Fanout card movement from slot *{0}* to slot *{1}* has started.**

Explanation

Substitution variables are:

*{0}*From location
*{1}*To location

Messages 1301-1400

1301 **Fanout card movement from slot *{0}* to slot *{1}* was successful.**

Explanation

Substitution variables are:

*{0}*From location
*{1}*To location

1302 **Fanout card movement from slot *{0}* to slot *{1}* failed.**

Explanation

Substitution variables are:

*{0}*From location
*{1}*To location

1303 **There were *{0}* STI paths swapped to their alternate paths for the fanout card in slot *{1}*.**

Explanation

Substitution variables are:

*{0}*Number of STI paths
*{1}*Location

1304 **There were *{0}* STI paths swapped to their default paths for the fanout card in slot *{1}*.**

Explanation

Substitution variables are:

*{0}*Number of STI paths
*{1}*Location

1305 **The group profile *{0}* was created.**

Explanation

Substitution variables are:

*{0}*Profile name

1306 **The group profile *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*Profile name

1307 **The group profile *{0}* was upgraded.**

Explanation

Substitution variables are:

*{0}*Profile name

1308 **The group profile *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*Profile name

1309 **The group profile *{0}* was imported.**

Explanation

Substitution variables are:

*{0}*Profile name

1310 **The *{0}* group was created by user *{1}*.**

Explanation

Substitution variables are:

*{0}*Group name
*{1}*User name

1311 **The *{0}* group was deleted by user *{1}*.**

Explanation

Substitution variables are:

*{0}*Group name
*{1}*User name

1312 **The associated activation profile for *{0}* in group *{1}* has been changed to *{2}*.**

Explanation

Substitution variables are:

*{0}*Managed object
*{1}*Group name
*{2}*Activation profile name

1313 **ID *{0}* was released from logical partition *{1}* by user *{3}*.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*Image name
*{2}*User name

1314 **ID *{0}* was configured off from logical partition *{1}* by user *{3}*.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*Image name
*{2}*User name

1315 **An attempt to reassign ID *{0}* from logical partition *{1}* to logical partition *{2}* by user *{3}* failed.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*Image name
*{2}*Image name
*{3}*User name

1316 **ID *{0}* was reassigned from logical partition *{1}* to logical partition *{2}* by user *{3}*.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*Image name
*{2}*Image name
*{3}*User name

1317 **ID *{0}* was released from logical partition *{1}*.**

Explanation

Substitution variables are:

*{0}*CHPID type
*{1}*Image name

1318 **A *{0}* operation was started by *{1}* from *{2}.{3}*.**

Explanation

Substitution variables are:

*{0}*Function name
*{1}*Origin console (User name)
*{2}*Network ID
*{3}*NAU

1319 **Channel LICCC update done on FRU location *{0}*. Original number of ports was *{1}*, new number of ports is *{2}*.**

Explanation

Substitution variables are:

*{0}*FRU location
*{1}*Old number of ports
*{2}*New number of ports

1320 **Customize Network Traffic Authorization: Allow Support Element LAN analysis = *{0}*, Allow SE OP sys analysis = *{1}*.**

Explanation

Substitution variables are:

{0}'1' if allowed, '0' if not allowed
{1}'1' if allowed, '0' if not allowed

1321 **Network traffic analysis for PCHID *{0}* set to own partition.**

Explanation

Substitution variables are:

*{0}*PCHID number

1322 **Network traffic analysis for PCHID *{0}* set to all partitions.**

Explanation

Substitution variables are:

*{0}*PCHID number

1323 **Network traffic analysis for PCHID *{0}* set to stop.**

Explanation

Substitution variables are:

*{0}*PCHID number

1324 **User *{0}* has been disabled for *{1}* minutes because of too many invalid logon attempts.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Number of minutes user logon is disabled

1325 **User *{0}* is no longer disabled from logging on.**

Explanation

Substitution variables are:

*{0}*User name

1326 **The managed objects role *{0}* has been deleted.**

Explanation

Substitution variables are:

*{0}*Role name

1327 **The task role *{0}* has been deleted.**

Explanation

Substitution variables are:

*{0}*Role name

1328 **The time zone was changed from *{0}* to *{1}*.**

Explanation

Substitution variables are:

*{0}*Old time zone
*{1}*New time zone

1329 **The time zone is currently set to *{0}*.**

Explanation

Substitution variables are:

*{0}*Time zone

1330 **The security log is within *{0}* percent of the maximum size; it should be archived to avoid loss of data.**

Explanation

Substitution variables are:

*{0}*Percentage of available space

1331 **The user *{0}* logged into the underlying console operating system platform.**

Explanation

Substitution variables are:

*{0}*User name

1332 **The user *{0}* logged out of the underlying console operating system platform.**

Explanation

Substitution variables are:

*{0}*User name

1333 **The console internal firewall blocked an incoming packet from *{0}* for port *{1}* using protocol *{2}*.**

Explanation

Substitution variables are:

*{0}*Origin machine
*{1}*Port number

*{2}*Protocol

1334 **A concurrent CP upgrade was performed. Current number of *{1}* are *{0}*.**

Explanation

Substitution variables are:

*{0}*Processor type
*{1}*Number of processors

1335 **Logical partition group control settings were changed.**

1336 **The backup file was written to the backup destination by Hardware Management Console *{0}***

Explanation

Substitution variables are:

*{0}*HMC Network ID.NAU

1337 **There was an ERROR writing the backup file to the backup destination using Hardware Management Console *{0}***

Explanation

Substitution variables are:

*{0}*HMC Network ID.NAU

1338 **Exclusive control was enabled by user *{0}*.**

Explanation

Substitution variables are:

*{0}*User name

1339 **Exclusive control was disabled by user *{0}*.**

Explanation

Substitution variables are:

*{0}*User name

1340 **An attempt for user *{0}* to log on failed.**

Explanation

Substitution variables are:

*{0}*User name

1341 **The user profile *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*User profile name

1342 **Start system anchor record upgrade.**

1343 **System anchor record upgrade was successful.**

1344	**System anchor record upgrade was cancelled.**
1345	**System anchor record upgrade was partially successful.**
1346	**System anchor record upgrade failed.**
1347	**Start permanent entitlement record upgrade.**
1348	**Permanent entitlement record upgrade was successful.**
1349	**Permanent entitlement record upgrade was cancelled.**
1350	**Permanent entitlement record upgrade was partially successful.**
1351	**Permanent entitlement record upgrade failed.**
1352	**Start temporary entitlement record upgrade for record ID *{0}*.**

Explanation

Substitution variables are:

*{0}*Record identifier

1353	**Temporary entitlement record upgrade was successful.**
1354	**Temporary entitlement record upgrade was cancelled.**
1355	**Temporary entitlement record upgrade was partially successful.**
1356	**Temporary entitlement record upgrade failed.**
1357	**Start channel LICCCC upgrade.**
1358	**Channel LICCCC upgrade was successful.**
1359	**Channel LICCCC upgrade was cancelled.**
1360	**Channel LICCCC upgrade was partially successful.**
1361	**Channel LICCCC upgrade failed.**
1362	**Start DIMM upgrade.**
1363	**DIMM upgrade was successful.**
1364	**DIMM upgrade was cancelled.**
1365	**DIMM upgrade was partially successful.**
1366	**DIMM upgrade failed.**
1367	**Permanent entitlement record is being staged**
1368	**Permanent entitlement record was staged successfully**
1369	**Permanent entitlement record failed to stage.**
1370	**The staged permanent entitlement record is being deleted.**
1371	**The staged permanent entitlement record has been deleted.**
1372	**The staged permanent entitlement record failed to delete.**
1373	**Temporary entitlement record is being staged**
1374	**Temporary entitlement record was staged successfully**
1375	**Temporary entitlement record failed to stage.**
1376	**The staged temporary entitlement record *{0}* is being deleted.**

Explanation

Substitution variables are:

*{0}*Record identifier

1377	**The staged temporary entitlement record has been deleted.**
1378	**The staged temporary entitlement record failed to delete.**
1379	**Activation of a temporary entitlement record *{0}* has started.**

Explanation

Substitution variables are:

*{0}*Record identifier

1380	**Activation of a temporary entitlement record was successful.**
1381	**Activation of a temporary entitlement record was cancelled.**
1382	**Activation of a temporary entitlement record was partially successful.**
1383	**Activation of a temporary entitlement record failed.**
1384	**Removal of the temporary entitlement record ID *{0}* has started.**

Explanation

Substitution variables are:

*{0}*Record identifier

1385	**Removal of a temporary entitlement record was successful.**
1386	**Removal of a temporary entitlement record failed.**
1387	**Processors are pending activation when available.**
1388	**Partition *{0}* has been assigned to use media on *{1}* by user *{2}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*NAU : User name
*{2}*User name

1389	**Partition *{0}* is no longer assigned to media on *{1}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*NAU : User name

1390	**Partition *{0}* is no longer assigned to media on *{1}* by request of user *{2}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*NAU : User name

*{2}*User name

1391 **Preload save upgrade data from the primary Support Element to the alternate Support Element started.**

1392 **Preload save upgrade data from the primary Support Element to the alternate Support Element completed successfully.**

1393 **Preload save upgrade data from the primary Support Element to the alternate Support Element failed. *{0}***

Explanation

Substitution variables are:

*{0}*Reason for the failure

1394 **The zeroize of usage domain *{0}* for cryptographic number *{1}* in logical partition *{2}* was successful.**

Explanation

Substitution variables are:

*{0}*Usage domain
*{1}*Cryptographic number
*{2}*Image name

1395 **The zeroize of usage domain(s) *{0}* for cryptographic number *{1}* was successful.**

Explanation

Substitution variables are:

*{0}*Usage domains
*{1}*Cryptographic number

1396 **The zeroize of usage domain *{0}* for cryptographic number *{1}* in logical partition *{2}* is deferred until configured online.**

Explanation

Substitution variables are:

*{0}*Usage domain
*{1}*Cryptographic number
*{2}*Image name

1397 **Telephone number *{0}* is no longer available for call-home connectivity. A new one should be configured.**

Explanation

Substitution variables are:

*{0}*Telephone number

1398 **Cryptographic controls were changed for active partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

1399 **Logical processor settings were changed for active partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

1400 **The code load was successful, but the Support Element could not connect back to the Hardware Management Console to send final report.**

Messages 1401-1500

1401 **Configuration data was copied to the USB memory stick.**

1402 **Retrieving a permanent entitlement record from support system.**

1403 **Retrieval of a permanent entitlement record from support system was successful.**

1404 **Retrieval of a permanent entitlement record from support system failed.**

1405 **Retrieving a temporary entitlement record from support system.**

1406 **Retrieval of a temporary entitlement record from support system was successful.**

1407 **Retrieval of a temporary entitlement record from support system failed.**

1408 **User *{0}* has *{1}* from *{2}* to session id *{4}* using password authentication method *{6}*.**

Explanation

Substitution variables are:

*{0}*User name
{1}'logged on' or 'reconnected'
{2}'the console', or the IP address of the user interface, or 'an unknown location'
*{4}*Logon session identifier
*{6}*the authentication method for the user's password of 'local' or 'LDAP'

1409 **User *{0}* has *{1}* from session id *{2}* for the reason: *{3}***

Explanation

Substitution variables are:

*{0}*User name
{1}'logged off' or 'disconnected'
*{2}*Logon session identifier
*{3}*Reason why the session was logged off or disconnected

1410 **User *{0}* of session *{1}* has forcibly *{2}* user *{3}* of session *{4}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Logon session identifier
{2}'logged off' or 'disconnected'
*{3}*Forced off user name
*{4}*Forced off logon session identifier

1411 **Hardware Management Console *{0}* is unable to be used as a call home server because it has no customer information configured.**

Explanation

Substitution variables are:

*{0}*HMC name

1412 **The following disruptive operation started: Activate. It was requested by *{0}* from *{1}*. *{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1413 **The following disruptive operation started: Configure channel off. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1414 **The following operation started: Concurrent switch. It was requested by *{0}* from *{1}*. *{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1415 **The following operation started: Disruptive switch. It was requested by *{0}* from *{1}*. *{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1416 **The following disruptive operation started: Deactivate. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1417 **The following disruptive operation started: Disable concurrent patch. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1418 **The following disruptive operation started: Install code changes/activate. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1419 **The following disruptive operation started: Load. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1420 **The following disruptive operation started: Power off. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1421 **The following disruptive operation started: Power-on reset. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1422 **The following disruptive operation started: PSW restart. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1423 **The following disruptive operation started: Remove code changes/activate. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1424 **The following disruptive operation started: Reset I/O Interface. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1425 **The following disruptive operation started: Run checkout tests. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1426 **The following disruptive operation started: Set clock. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1427 **The following disruptive operation started: Stop. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1428 **The following disruptive operation started: Sysplex timer configuration change. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1429 **The following disruptive operation started: System reset. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{5}.{6}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1430 **The following disruptive operation started: System reset normal for object *{0}*. It was requested by *{1}* from *{2}.{3}* at IP address *{4}*. At this time, the user was using single object operation from *{5}.{6}*.**

Explanation

Substitution variables are:

*{0}*Target object name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Origin IP address
*{5}*Single object operation Network ID
*{6}*Single object operation NAU

1431 **The following disruptive operation started: System reset clear for object *{0}*. It was requested by *{1}* from *{2}.{3}* at IP address *{4}*. At this time, the user was using single object operation from *{5}.{6}*.**

Explanation

Substitution variables are:

*{0}*Target object name
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Origin IP address
*{5}*Single object operation Network ID
*{6}*Single object operation NAU

1432 **The following disruptive operation started: Unknown. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

1433 **The following disruptive operation started: Activate. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1434 **The following disruptive operation started: Configure channel off. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU

*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1435 **The following operation started: Concurrent switch. It was requested by *{0}* from *{1}*. *{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1436 **The following operation started: Disruptive switch. It was requested by *{0}* from *{1}*. *{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1437 **The following disruptive operation started: Deactivate. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1438 **The following disruptive operation started: Disable concurrent patch. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1439 **The following disruptive operation started: Install code changes/activate. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1440 **The following disruptive operation started: Load. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1441 **The following disruptive operation started: Power off. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU

*{6}*Single object operation IP address

1442 **The following disruptive operation started: Power-on reset. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1443 **The following disruptive operation started: PSW restart. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1444 **The following disruptive operation started: Remove code changes/activate. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1445 **The following disruptive operation started: Reset I/O Interface. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type

*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1446 **The following disruptive operation started: Run checkout tests. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1447 **The following disruptive operation started: Set clock. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1448 **The following disruptive operation started: Stop. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1449 **The following disruptive operation started: Sysplex Timer configuration change. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1450 **The following disruptive operation started: System reset. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{7}*) was using single object operation from *{5}.{6}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1451 **The following disruptive operation started: System reset normal for object *{0}*. It was requested by *{1}* from *{2}.{3}* at IP address *{4}*. At this time, the user (at IP address *{7}*) was using single object operation from *{5}.{6}*.**

Explanation

Substitution variables are:

*{0}*Target
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Origin IP address
*{5}*Single object operation Network ID
*{6}*Single object operation NAU
*{7}*Single object operation IP address

1452 **The following disruptive operation started: System reset clear for object *{0}*. It was requested by *{1}* from *{2}.{3}* at IP address *{4}*. At this time, the user (at IP address *{7}*) was using single object operation from *{5}.{6}*.**

Explanation

Substitution variables are:

*{0}*Target
*{1}*Interface type
*{2}*Origin Network ID
*{3}*Origin NAU
*{4}*Origin IP address

*{5}*Single object operation Network ID
*{6}*Single object operation NAU
*{7}*Single object operation IP address

1453 **The following disruptive operation started: Unknown. It was requested by *{0}* from *{1}.{2}* at IP address *{3}*. At this time, the user (at IP address *{6}*) was using single object operation from *{4}.{5}*.**

Explanation

Substitution variables are:

*{0}*Interface type
*{1}*Origin Network ID
*{2}*Origin NAU
*{3}*Origin IP address
*{4}*Single object operation Network ID
*{5}*Single object operation NAU
*{6}*Single object operation IP address

1454 **Blocking of automatic microcode installation has been *{0}* by *{1}* logged on from location *{2}*.**

Explanation

Substitution variables are:

*{0}*Enabled or disabled
*{1}*User name
*{2}*IP address or host name [IP address] if host name differs from IP address

1455 **The operating system upgrade was successful.**

1456 **The operating system upgrade encountered a problem copying system files from /bom directory.**

1457 **User *{0}* of session *{1}* has switched from user interface "*{2}*" to "*{3}*".**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Logon session identifier
*{2}*Old user interface style
*{3}*New user interface style

1458 **Prepare system for discontinuance started**

1459 **Prepare system for discontinuance ended with errors**

1460 **Prepare system for discontinuance ended**

1461 **Cleanup discontinuance started**

1462 **Cleanup discontinuance ended with errors**

1463 **Cleanup discontinuance ended**

1464 **Send processor change notification started**

1465 **Send processor change notification ended with errors**

1466 **Send processor change notification ended**

1467	**Data Replication being enabled**
1468	**Data Replication being disabled**
1469	**The following internal code changes were retrieved from hard drive by user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1470	**The following internal code changes were installed by user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1471	**The following internal code changes were removed by user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1472	**The following internal code changes were accepted by user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1473	**The following internal code changes were deleted by user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1474	**The following internal code changes were retrieved from mass storage media by user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1475	**The following internal code changes were retrieved from the server by user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1476 **A failure occurred retrieving the following internal code changes for user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1477 **A failure occurred installing the following internal code changes for user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1478 **A failure occurred deleting the following internal code changes for user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1479 **A failure occurred removing the following internal code changes for user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1480 **A failure occurred accepting the following internal code changes for user *{0}*: *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*MCL levels

1481 **The reset profile *{0}* was created. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU

1482 **The load profile *{0}* was created. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU

1483 **The image profile *{0}* was created. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU

1484 **The system activity profile *{0}* was created. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU

1485 **The reset profile *{0}* was changed. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU

1486 **The load profile *{0}* was changed. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU

1487 **The image profile *{0}* was changed. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU

1488 **The system activity profile *{0}* was changed. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID

*{2}*NAU

1489 **The reset profile *{0}* was upgraded. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU

1490 **The load profile *{0}* was upgraded. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU

1491 **The image profile *{0}* was upgraded. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU

1492 **The system activity profile *{0}* was upgraded. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU

1493 **The reset profile *{0}* was deleted. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU

1494 **The load profile *{0}* was deleted. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU

1495 **The image profile *{0}* was deleted. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU

1496 **The system activity profile *{0}* was deleted. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU

1497 **The reset profile *{0}* was imported. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU

1498 **The load profile *{0}* was imported. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU

1499 **The image profile *{0}* was imported. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU

1500 **The system activity profile *{0}* was imported. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU

Messages 1501-1600

1501 **The reset profile *{0}* was created. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1502 **The load profile *{0}* was created. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1503 **The image profile *{0}* was created. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1504 **The system activity profile *{0}* was created. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1505 **The reset profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1506 **The load profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1507 The image profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1508 The system activity profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1509 The reset profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1510 The load profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1511 The image profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID

*{2}*NAU
*{3}*Interface requesting the change

1512 The system activity profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1513 The reset profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1514 The load profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1515 The image profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1516 The system activity profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1517 The reset profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1518 **The load profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1519 **The image profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1520 **The system activity profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1521 **The reset profile *{0}* was created. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1522 **The load profile *{0}* was created. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1523 **The image profile *{0}* was created. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1524 **The system activity profile *{0}* was created. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1525 **The reset profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1526 **The load profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1527 **The image profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1528 **The system activity profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1529 **The reset profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1530 **The load profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1531 **The image profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name

*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1532 **The system activity profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1533 **The reset profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1534 **The load profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1535 **The image profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1536 **The system activity profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1537 **The reset profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1538 **The load profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1539 **The image profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1540 **The system activity profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

*{4}*Origin IP address

1542 The group profile *{0}* was created. It was requested from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU

1543 The group profile *{0}* was changed. It was requested from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU

1544 The group profile *{0}* was upgraded. It was requested from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU

1545 The group profile *{0}* was deleted. It was requested from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU

1546 The group profile *{0}* was imported. It was requested from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU

1547 The group profile *{0}* was created. It was requested by *{3}* from *{1}.{2}*.

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1548 **The group profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1549 **The group profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1550 **The group profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1551 **The group profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change

1552 **The group profile *{0}* was created. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1553 **The group profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1554 **The group profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1555 **The group profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1556 **The group profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*Interface requesting the change
*{4}*Origin IP address

1557 **The reset profile *{0}* was created. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Reset profile name

1558 **The load profile *{0}* was created. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Load profile name

1559 **The image profile *{0}* was created. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Image profile name

1560 **The system activity profile *{0}* was created. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*System activity profile name

1561 **The group profile *{0}* was created. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name

1562 **The reset profile *{0}* was changed. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Reset profile name

1563 **The load profile *{0}* was changed. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Load profile name

1564 **The image profile *{0}* was changed. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Image profile name

1565 **The system activity profile *{0}* was changed. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*System activity profile name

1566 **The group profile *{0}* was changed. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name

1567 **The reset profile *{0}* was upgraded. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Reset profile name

1568 **The load profile *{0}* was upgraded. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Load profile name

1569 **The image profile *{0}* was upgraded. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Image profile name

1570 **The system activity profile *{0}* was upgraded. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*System activity profile name

1571 **The group profile *{0}* was upgraded. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name

1572 **The reset profile *{0}* was deleted. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Reset profile name

1573 **The load profile *{0}* was deleted. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Load profile name

1574 **The image profile *{0}* was deleted. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Image profile name

1575 **The system activity profile *{0}* was deleted. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*System activity profile name

1576 **The group profile *{0}* was deleted. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name

1577 **The reset profile *{0}* was imported. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Reset profile name

1578 **The load profile *{0}* was imported. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Load profile name

1579 **The image profile *{0}* was imported. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*Image profile name

1580 **The system activity profile *{0}* was imported. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*System activity profile name

1581 **The group profile *{0}* was imported. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name

1582 **The reset profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}*. *{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1583 **The load profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1584 **The image profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1585 **The system activity profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1586 **The group profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1587 **The reset profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1588 **The load profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1589 **The image profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1590 **The system activity profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1591 **The group profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1592 **The reset profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1593 **The load profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1594 **The image profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1595 **The system activity profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1596 **The group profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1597 **The reset profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1598 **The load profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1599 **The image profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1600 **The system activity profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

Messages 1601-1700

1601 **The group profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1602 **The reset profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}*.*{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1603 **The load profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1604 **The image profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1605 **The system activity profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1606 **The group profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1607 **The reset profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1608 **The load profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1609 **The image profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1610 **The system activity profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1611 **The group profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1612 **The reset profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1613 **The load profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1614 **The image profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1615 **The system activity profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1616 **The group profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1617 **The reset profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1618 **The load profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1619 **The image profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1620 **The system activity profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1621 **The group profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1622 **The reset profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1623 **The load profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1624 **The image profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1625 **The system activity profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1626 **The group profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1627 **The reset profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1628 **The load profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1629 **The image profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1630 **The system activity profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1631 **The group profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1632 **The reset profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1633 **The load profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}*.*{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1634 **The image profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}*.*{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1635 **The system activity profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}*.*{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1636 **The group profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}*.*{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

*{4}*Origin IP address

1637 **The reset profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1638 **The load profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1639 **The image profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1640 **The system activity profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1641 **The group profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1642 **The reset profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1643 **The load profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1644 **The image profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1645 **The system activity profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1646 **The group profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1647 **The reset profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1648 **The load profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1649 **The image profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1650 **The system activity profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name

*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1651 **The group profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1652 **The reset profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1653 **The load profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1654 **The image profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1655 **The system activity profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1656 **The group profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1657 **The reset profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1658 **The load profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1659 **The image profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

*{4}*Origin IP address

1660 **The system activity profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1661 **The group profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1662 **The reset profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1663 **The load profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1664 **The image profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1665 **The system activity profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1666 **The group profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1667 **The reset profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1668 **The load profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1669 **The image profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1670 **The system activity profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1671 **The group profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1672 **The reset profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1673 **The load profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name

*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1674 **The image profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1675 **The system activity profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1676 **The group profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1677 **The reset profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Reset profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1678 **The load profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Load profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1679 **The image profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*Image profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1680 **The system activity profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*System activity profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1681 **The group profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR group profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1682 **The server *{0}* with key type *{1}* was added to the Network Time Protocol (NTP) configuration file.**

Explanation

Substitution variables are:

*{0}*NTP server name
*{1}*Key type of the NTP server

1683 **The server *{0}* with key type *{1}* and symmetric key value *{2}* was added to the Network Time Protocol (NTP) configuration file.**

Explanation

Substitution variables are:

*{0}*NTP server name
*{1}*Key type of the NTP server
*{2}*Symmetric key value of the NTP server

1684 **The server *{0}* was removed from the Network Time Protocol (NTP) configuration file.**

Explanation

Substitution variables are:

*{0}*NTP server name

1685 **The server *{0}* version *{1}* was removed from the Network Time Protocol (NTP) configuration file.**

Explanation

Substitution variables are:

*{0}*NTP server name
*{1}*Key type of the NTP server

1686 **The console has been enabled as a Network Time Protocol (NTP) client.**

1687 **The console is no longer enabled as a Network Time Protocol (NTP) client.**

1688 **The console has been enabled as a Network Time Protocol (NTP) server.**

1689 **The console is no longer enabled as a Network Time Protocol (NTP) server.**

1690 **The Network Time Protocol (NTP) service has detected an error and disabled itself.**

1691 **User *{0}* has attempted to log on from location *{1}* with a user identification or password that was not valid.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*IP address

1692 **An attempt for user *{0}* to log on from location *{1}* failed.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*IP address

1693 **Logical partition weight settings were changed by a scheduled operation.**

1694 **The Support Element's service call logical processor event manager attempted, but could not send configuration management data (event type 04) to the following system(s): *{0}*.**

Explanation

Substitution variables are:

*{0}*Image names

1695	**Concurrent upgrade Engineering Changes (EC) activate of system EC *{0}* completed, but not all functions may be available until the next system activation. Additionally, one or more active partitions did not respond to new function notification.**

Explanation

Substitution variables are:

*{0}*System EC number

1696	**Concurrent upgrade Engineering Changes (EC) activate of system EC *{0}* completed, All functions are available but one or more active partitions did not respond to new function notification.**

Explanation

Substitution variables are:

*{0}*System EC number

1697	**Temporary On/Off CoD resources were converted to permanent resources during power-on reset**
1698	**Start add I/O drawer phase 1.**
1699	**Add I/O drawer phase 1 was successful.**
1700	**Add I/O drawer phase 1 failed.**

Messages 1701-1800

1701	**Start add I/O drawer phase 2.**
1702	**Add I/O drawer phase 2 was successful.**
1703	**Add I/O drawer phase 2 failed.**
1704	**Start remove I/O drawer phase 1.**
1705	**Remove I/O drawer phase 1 was successful.**
1706	**Remove I/O drawer phase 1 failed.**
1707	**Start remove I/O drawer phase 2.**
1708	**Remove I/O drawer phase 2 was successful.**
1709	**Remove I/O drawer phase 2 failed.**
1710	**Battery operated clock old time (prior to turning on network time protocol).**
1711	**A Change LPAR controls scheduled operation was started from *{0}.{1}*.**

Explanation

Substitution variables are:

*{0}*NAU
*{1}*Network ID

1712	**Network traffic analysis for PCHID *{0}* port *{1}* set to own partition.**

Explanation

Substitution variables are:

*{0}*PCHID name
*{1}*Port number

1713 **Network traffic analysis for PCHID *{0}* port *{1}* set to all partitions.**

Explanation

Substitution variables are:

*{0}*PCHID name
*{1}*Port number

1714 **Network traffic analysis for PCHID *{0}* port *{1}* set to all data on port.**

Explanation

Substitution variables are:

*{0}*PCHID name
*{1}*Port number

1715 **Network traffic analysis for PCHID *{0}* port *{1}* set to stop.**

Explanation

Substitution variables are:

*{0}*PCHID name
*{1}*Port number

1716 **Start permanent entitlement record pre-check.**

1717 **Permanent entitlement record pre-check was successful.**

1718 **Permanent entitlement record pre-check was cancelled.**

1719 **Permanent entitlement record pre-check was partially successful.**

1720 **Permanent entitlement record pre-check failed.**

1731 **HiperSockets network traffic analyzer authorization has changed.**

1732 **HiperSockets network traffic analyzer authorization has been disabled.**

1733 **The LPAR control profile *{0}* was created.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name

1734 **The LPAR control profile *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name

1735 **The LPAR control profile *{0}* was upgraded.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name

1736 **The LPAR control profile *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name

1737 **The LPAR control profile *{0}* was imported.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name

1738 **The LPAR control profile *{0}* was created. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU

1739 **The LPAR control profile *{0}* was changed. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU

1740 **The LPAR control profile *{0}* was upgraded. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU

1741 **The LPAR control profile *{0}* was deleted. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU

1742 **The LPAR control profile *{0}* was imported. It was requested from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU

1743 **The LPAR control profile *{0}* was created. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1744 **The LPAR control profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1745 **The LPAR control profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1746 **The LPAR control profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1747 **The LPAR control profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU

*{3}*User name

1748 **The LPAR control profile *{0}* was created. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1749 **The LPAR control profile *{0}* was changed. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1750 **The LPAR control profile *{0}* was upgraded. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1751 **The LPAR control profile *{0}* was deleted. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1752 **The LPAR control profile *{0}* was imported. It was requested by *{3}* from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1753 **The LPAR control profile *{0}* was created. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name

1754 **The LPAR control profile *{0}* was changed. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name

1755 **The LPAR control profile *{0}* was upgraded. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name

1756 **The LPAR control profile *{0}* was deleted. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name

1757 **The LPAR control profile *{0}* was imported. It was requested by Support Element LIC.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name

1758 **The LPAR control profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1759 **The LPAR control profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1760 **The LPAR control profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1761 **The LPAR control profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1762 **The LPAR control profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1763 **The LPAR control profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1764 **The LPAR control profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1765 **The LPAR control profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1766 **The LPAR control profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1767 **The LPAR control profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

1768 **The LPAR control profile *{0}* was created. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1769 **The LPAR control profile *{0}* was changed. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1770 **The LPAR control profile *{0}* was upgraded. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1771 **The LPAR control profile *{0}* was deleted. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1772 **The LPAR control profile *{0}* was imported. It was requested by Support Element(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1773 **The LPAR control profile *{0}* was created. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name

*{4}*Origin IP address

1774 **The LPAR control profile *{0}* was changed. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1775 **The LPAR control profile *{0}* was upgraded. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1776 **The LPAR control profile *{0}* was deleted. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1777 **The LPAR control profile *{0}* was imported. It was requested by Hardware Management Console(*{3}*) from *{1}.{2}* at IP address *{4}*.**

Explanation

Substitution variables are:

*{0}*LPAR control profile name
*{1}*Network ID
*{2}*NAU
*{3}*User name
*{4}*Origin IP address

1778 **A change LPAR controls scheduled operation failed. The request for the following partition(s) resulted in a WLM / capping conflict:\n *{0}***

Explanation

Substitution variables are:

*{0}*Image names

1779 **The user *{0}* opened an ssh session into the underlying console operating system platform from *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*HMC name

1780 **The user *{0}* ssh session closed.**

Explanation

Substitution variables are:

*{0}*User name

1781 **RSF diagnostic test trace output was saved as *{0}*.**

Explanation

Substitution variables are:

*{0}*File name of the TCP dump

1782 **The static power savings mode for this system has been enabled.**

1783 **The static power savings mode for this system has been disabled.**

1790 **LPAR controls profiles were exported.**

1791 **LPAR controls profiles were imported.**

1800 **RSF diagnostic query size operation detected *{0}* MCL files totalling *{1}* bytes.**

Explanation

Substitution variables are:

*{0}*Number of MCL files
*{1}*Number of bytes in all MCL files

Messages 1801-1900

1801 **The user template *{0}* was added.**

Explanation

Substitution variables are:

*{0}*Template name

1802 **The user template *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*Template name

1803 **The user template *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*Template name

1804 **The process to copy a backup file to backup media is about to start *{0}* .**

Explanation

Substitution variables are:

*{0}*Information about the backup file and backup media.

1805 **Concurrent internal code changes for PU core started.**

1806 **Concurrent internal code changes for PU core completed.**

1807 **Concurrent internal code changes for PU core failed.**

1808 **The console has been enabled as a Network Time Protocol (NTP) client. This message was recorded *{0}* seconds after the previous NTP message.**

Explanation

Substitution variables are:

*{0}*Number seconds

1809 **Power Cap settings have changed.**

1810 **The activation of an incompatible UDX image for cryptographic coprocessor *{0}* was successfully forced. Timestamp: *{1}*, Name: *{2}***

Explanation

Substitution variables are:

*{0}*Cryptographic number
*{1}*Timestamp
*{2}*UDX image name

1811 **The activation of the factory default image for cryptographic coprocessor *{0}* was successfully forced.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

1812 **Replenishment of the temporary entitlement record ID *{0}* has started.**

Explanation

Substitution variables are:

*{0}*Temporary entitlement record identifier

1813 **Replenishment of the temporary entitlement record ID *{0}* was successful.**

Explanation

Substitution variables are:

*{0}*Temporary entitlement record identifier

1814 **Replenishment of the Temporary entitlement record ID *{0}* failed.**

Explanation

Substitution variables are:

*{0}*Temporary entitlement record identifier

1848 **The pending activation of the factory default image for cryptographic coprocessor *{0}* was successfully cancelled.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

1849 **The following systems are not entitled for remote service: *{0}*.**

Explanation

Substitution variables are:

*{0}*Machine type and machine serial number of all systems not entitled.

1851 **Extracting and validating file *{0}* using key for family *{1}***

Explanation

Substitution variables are:

*{0}*PK1 file name
*{1}*Machine family

1852 **The user pattern *{0}* was added.**

Explanation

Substitution variables are:

*{0}*Pattern name

1853 **The user pattern *{0}* was deleted.**

Explanation

Substitution variables are:

*{0}*Pattern name

1854 **The user pattern *{0}* was changed.**

Explanation

Substitution variables are:

*{0}*Pattern name

1883 **Power save enabled.**

1889 **Battery-operated clock has been adjusted by *{0}* milliseconds over the last *{1}* hours.**

Explanation

Substitution variables are:

*{0}*Number of milliseconds time was adjusted
*{1}*Time was adjusted over the last hours

1890 **Unable to obtain time from the CPC. The battery-operated clock for this console might not be accurate.**

1891 **Battery-operated clock has been adjusted by *{0}* milliseconds.**

Explanation

Substitution variables are:

*{0}*Number of milliseconds time was adjusted

1892 **Battery-operated clock has been adjusted by *{0}* millisecond over the last *{1}* hours.**

Explanation

Substitution variables are:

*{0}*Number of milliseconds time was adjusted
*{1}*Amount of time that was adjusted over the last hours

1893 **Battery-operated clock has been adjusted by *{0}* milliseconds over the last hour.**

Explanation

Substitution variables are:

*{0}*Number of milliseconds time was adjusted

1894 **Battery-operated clock has been adjusted by *{0}* millisecond over the last hour.**

Explanation

Substitution variables are:

*{0}*Number of milliseconds time was adjusted

1895 **Battery-operated clock has been adjusted by *{0}* millisecond.**

Explanation

Substitution variables are:

*{0}*Number of milliseconds time was adjusted

1896 **The shared memory used by the backup has been already released.**

Messages 1901-2000

1915 **Service data was sent to the support system. It was associated to *{0}* *{1}*.**

Explanation

Substitution variables are:

*{0}*Problem type
*{1}*Problem number

1916 **CPC Firmware embedded framework control code load started.**

1917 **CPC Firmware embedded framework control code load completed successfully.**

1918 **CPC Firmware embedded framework control code load failed.**

1919	**Concurrent internal code changes for CPC firmware embedded framework control code started.**
1920	**Concurrent internal code changes for CPC firmware embedded framework control code completed.**
1921	**Concurrent internal code changes for CPC firmware embedded framework control code failed.**
1922	**Activation of this image was not performed.**
1923	**Software Maintenance Agreement (SWMA) has been validated.**
1924	**The firmware network adapter parameters were created for image *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

1925	**The firmware network adapter parameters were changed for image *{0}*.**

Explanation

Substitution variables are:

*{0}*Image name

1926	**The configuration type of cryptographic number *{0}* has been changed to a cryptographic EP11 coprocessor.**

Explanation

Substitution variables are:

*{0}*Cryptographic number

1927	**Start Feature on demand update.**
1928	**Feature on demand update was successful.**
1929	**Feature on demand update was cancelled.**
1930	**Feature on demand update was partially successful.**
1931	**Feature on demand update failed.**
1932	**Feature on demand record is being staged**
1933	**Feature on demand record was staged successfully**
1934	**Feature on demand record failed to stage.**
1935	**The staged feature on demand record is being deleted.**
1936	**The staged feature on demand record has been deleted.**
1937	**The staged feature on demand record failed to delete.**
1938	**Removal of a feature on demand has started.**
1939	**Removal of a feature on demand was successful.**
1940	**Removal of a feature on demand failed.**
1941	**User *{0}* has logged on to Web Services API session *{1}* from location *{2}***

Explanation

Substitution variables are:

*{0}*User name
*{1}*Session log identifier
*{2}*IP address and possibly host name if host name can be determined. If a client tag was specified on the login attempt it is also provided here.

1942 **User *{0}* has logged off from Web Services API session *{1}* due to *{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Session log identifier
*{2}*Reason for logoff.

1943 **Modem is not supported on this version of the HMC. *{0}* is disabled.**

Explanation

Substitution variables are:

*{0}*Function that is no longer supported

1944 **Call-home has been disabled on this HMC. You must configure an internet connection to enable remote support.**

1945 **Check of on hold internal code changes has been *{0}* by *{1}* logged on from location *{2}*.**

Explanation

Substitution variables are:

*{0}*Enabled or disabled
*{1}*User name
*{2}*IP address and optional host name

1946 **Starting install of the following internal code changes: *{0}*.**

Explanation

Substitution variables are:

*{0}*Collections to install

1947 **Starting remove of the following internal code changes: *{0}*.**

Explanation

Substitution variables are:

*{0}*Collections to remove

1948 **Authentication KEY created on primary Support Element.**

1949 **Authentication KEY sent to the alternate Support Element.**

1950 **Authentication KEY restored from the alternate Support Element.**

1951 **A flash memory allocation was added for logical partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Logical partition name

1952 **A flash memory allocation was removed for logical partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Logical partition name

1953 **A flash memory allocation was changed for logical partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Logical partition name

1954 **Start remove I/O disruptively.**

1955 **Remove I/O disruptively was successful.**

1956 **Remove I/O disruptively failed.**

1957 **User *{0}* successfully logged on using pattern *{2}* with a template of *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*User pattern
*{2}*User template

1958 **Battery operated clock set to new time obtained directly from NTP server.**

1959 **Concurrent internal code changes for PCI support partition code started.**

1960 **Concurrent internal code changes for PCI support partition code completed.**

1961 **Concurrent internal code changes for PCI support partition code failed.**

1962 **The Monitor System Events task failed to send an email to *{0}* with a message count of *{1}* for sources *{2}* due to exception *{3}*.**

Explanation

Substitution variables are:

*{0}*Destination email address
*{1}*The index of the message in the queue
*{2}*Sources jcc, need a better description of Sources
*{3}*Description of the error

1964 **The current absolute capping value for the *{0}* CPs in partition *{1}* changed from *{2}* to *{3}*.**

Explanation

Substitution variables are:

*{0}*Type of CPs

*{1}*Image name
*{2}*Old absolute capping value
*{3}*New absolute capping value

1965 **The current absolute capping value for the *{0}* CPs in partition *{1}* changed from None to *{2}*.**

Explanation

Substitution variables are:

*{0}*Type of CPs
*{1}*Image name
*{2}*New absolute capping value

1966 **The current absolute capping value for the *{0}* CPs in partition *{1}* changed from *{2}* to None.**

Explanation

Substitution variables are:

*{0}*Type of CPs
*{1}*Image name
*{2}*Old absolute capping value

1967 **TSD request was sent to the Support Element**

1968 **Smart card has been inserted into Support Element.**

1969 **The file *{0}* is to large to be sent to the support system.**

Explanation

Substitution variables are:

*{0}*File name

1986 **The backup file is going to be written to a removable media.**

1987 **The backup file is going to be written to a FTP server.**

1989 **Task *{0}* with identifier *{1}* started by user *{2}* in session *{3}*.**

Explanation

Substitution variables are:

*{0}*Task name
*{1}*Unique task identifier
*{2}*User name
*{3}*Logon session identifier

1990 **Task *{0}* with identifier *{1}* started by user *{2}* in session *{3}*; targets are: *{4}***

Explanation

Substitution variables are:

*{0}*Task name
*{1}*Unique task identifier
*{2}*User name
*{3}*Logon session identifier

*{4}*Names of the targets for the task

1991 **Task *{0}* with identifier *{1}* for user *{2}* has ended.**

Explanation

Substitution variables are:

*{0}*Task name
*{1}*Unique task identifier
*{2}*User name

1992 **Start generic feature on demand update.**

1993 **Generic feature on demand update was successful.**

1994 **Generic feature on demand update was cancelled.**

1995 **Generic feature on demand update was partially successful.**

1996 **Generic feature on demand update failed.**

1997 **The remote service configuration data was updated.**

1998 **The user role *{0}* has been created.**

Explanation

Substitution variables are:

*{0}*User role name

1999 **The user role *{0}* has been changed.**

Explanation

Substitution variables are:

*{0}*User role name

2000 **The user role *{0}* has been deleted.**

Explanation

Substitution variables are:

*{0}*User role name

Messages 2001-2100

2001 **The user role *{0}* has been created.**

Explanation

Substitution variables are:

*{0}*User role name

2002 **The user role *{0}* has been changed.**

Explanation

Substitution variables are:

*{0}*User role name

2004 **Concurrent internal code changes for self boot engine started.**

2005 **Concurrent internal code changes for self boot engine completed.**

2006 **Concurrent internal code changes for self boot engine code failed.**

2007 **User *{0}* has acknowledged viewing license information.**

Explanation

Substitution variables are:

*{0}*User name

2008 **Start request was initiated for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

2009 **Start request has ended successfully for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

2010 **Start request has ended with failure for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

2011 **Stop request was initiated for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

2012 **Stop request has ended successfully for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

2013 **Stop request has ended with failure for system *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC name

2016 **Start request for system *{0}* was cancelled.**

Explanation

Substitution variables are:

*{0}*CPC name

2017	**Concurrent internal code changes for master control support partition started.**
2018	**Concurrent internal code changes for master control support partition completed.**
2019	**Concurrent internal code changes for master control support partition failed.**
2020	**Start request was initiated for partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Partition name

2021	**Start request has ended successfully for partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Partition name

2022	**Start request has ended with failure for partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Partition name

2023	**Stop request was initiated for partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Partition name

2024	**Stop request has ended successfully for partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Partition name

2025	**Stop request has ended with failure for partition *{0}*.**

Explanation

Substitution variables are:

*{0}*Partition name

2026	**Start request for partition *{0}* was cancelled.**

Explanation

Substitution variables are:

*{0}*Partition name

2027	**Stop request for system *{0}* was cancelled.**

Explanation

Substitution variables are:

*{0}*CPC name

2028 **A licensed internal code error detected by Hardware Management Console *{0}* caused the disablement of the installation and activation of internal code changes.**

Explanation

Substitution variables are:

*{0}*Origin HMC

2029 **User *{0}* of session *{1}* was switched from user interface "*{2}*" to "*{3}*" because Dynamic Partition Manager was enabled on a CPC *{4}* permitted to this user.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Logon session identifier
*{2}*Old user interface style
*{3}*New user interface style
*{4}*Names of the CPC's that forced the UI style change.

2030 **The zeroize of the cryptographic configuration was partially successful.**

2031 **User *{0}* was not permitted to log on since the userid is disabled due to inactivity.**

Explanation

Substitution variables are:

*{0}*User name

2032 **Virtual Flash Memory values for partition *{0}* are: *{1}* GB (initial), *{2}* GB (current), *{3}* GB (maximum).**

Explanation

Substitution variables are:

*{0}*Logical partition name
*{1}*initial Virtual Flash Memory amount
*{2}*current Virtual Flash Memory amount
*{3}*maximum Virtual Flash Memory amount

2033 **The shared secret key for user *{0}* has been reset.**

Explanation

Substitution variables are:

*{0}*User name

2034 **The cryptographic UDX image *{0}* was successfully imported from *{1}* using *{2}*.**

Explanation

Substitution variables are:

*{0}*UDX image name
*{1}*Host name
*{2}*FTP protocol type

2035 **The Mobile App preferences were changed by *{0}*. App enabled: *{1}* to *{2}* Require app password enabled: *{3}* to *{4}* Password caching enabled: *{5}* to *{6}* Actions enabled: *{7}* to *{8}* Actions settings: *{9}* to *{10}* Notifications enabled: *{11}* to *{12}***

Explanation

Substitution variables are:

*{0}*User name
*{1}*App enabled old value
*{2}*App enabled new value
*{3}*Require app password enabled old value
*{4}*Require app password enabled new value
*{5}*Password caching enabled old value
*{6}*Password caching enabled enabled new value
*{7}*Actions enabled old value
*{8}*Actions enabled new value
*{9}*Actions settings old value
*{10}*Actions settings new value
*{11}*Notifications enabled old value
*{12}*Notifications enabled new value

2036 **Notification preferences for the Mobile app were changed by *{0}* on device *{1}* for *{2}*. Notifications for this device are *{3}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Device token
*{2}*System name
{3}'disabled' or 'enabled'

2037 **All notification registrations cleaned for user *{0}*.**

Explanation

Substitution variables are:

*{0}*User name

2038 **All notification registrations cleaned for device *{0}*.**

Explanation

Substitution variables are:

*{0}*Device token

2039 **All notification registrations cleaned for system with serial number *{0}*.**

Explanation

Substitution variables are:

*{0}*CPC serial number

2040 **Power save disabled.**

2042 **User *{0}* has logged on to BCPii API session *{1}* from source *{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*API session identifier
*{2}*Name for the source of the request

2043 **User *{0}* has logged off from BCPii API session *{1}* due to *{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*API session identifier
*{2}*Reason for logoff

2044 **The system BCPii Permissions have been altered.**

2046 **The corresponding BCPii permissions for image profile *{0}*.**

Explanation

Substitution variables are:

*{0}*The image profile name.

2047 **The corresponding BCPii permissions entry *{1}* for image profile *{0}*.**

Explanation

Substitution variables are:

*{0}*The image profile name.
*{1}*The log entry number.

2048 **Multi-factor authentication has changed.**

2049 **The corresponding Change LPAR Security BCPii permissions for logical partition *{0}*.**

Explanation

Substitution variables are:

*{0}*The logical partition name.

2050 **The corresponding Change LPAR Security BCPii permissions entry *{1}* for logical partition *{0}*.**

Explanation

Substitution variables are:

*{0}*The logical partition name.
*{1}*The log entry number.

2051 **Concurrent internal code changes for EDiF appliance started.**

2052	**Concurrent internal code changes for EDiF appliance completed.**
2053	**Concurrent internal code changes for EDiF appliance failed.**
2054	**A CA certificate was added to the EDiF trust store for *{0}***

Explanation

Substitution variables are:

*{0}*SE name

2055	**A server certificate was added to the EDiF trust store for *{0}***

Explanation

Substitution variables are:

*{0}*SE name

2056	**A new CA signed certificate is now set as the active certificate for *{0}***

Explanation

Substitution variables are:

*{0}*SE name

2057	**A new self-signed certificate was created and set as the active certificate for *{0}***

Explanation

Substitution variables are:

*{0}*SE name

2058	**The wrapping key expiration was successfully changed from *{0}* to *{1}* on *{2}***

Explanation

Substitution variables are:

*{0}*old value
*{1}*new value
*{2}*SE name

2059	**A CA certificate was removed from the EDiF trust store**
2060	**A server certificate was removed from the EDiF trust store**
2061	**The link encryption required was changed from *{0}* to *{1}***

Explanation

Substitution variables are:

*{0}*old value
*{1}*new value

2062	**The link authentication required was successfully changed from *{0}* to *{1}* on *{2}***

Explanation

Substitution variables are:

*{0}*old value
*{1}*new value
*{2}*SE name

2063 **The session key expiration was successfully changed from *{0}* to *{1}***

Explanation

Substitution variables are:

*{0}*old value
*{1}*new value

2064 **A set of activation profiles was changed.**

2065 **A set of activation profiles was changed. It was requested from *{0}.{1}*.**

Explanation

Substitution variables are:

*{1}*Network ID
*{2}*NAU

2066 **A set of activation profiles was changed. It was requested by *{2}* from *{0}.{1}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name

2067 **A set of activation profiles was changed. It was requested by *{2}* from *{0}.{1}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name
*{3}*Origin IP address

2068 **A set of activation profiles was changed. It was requested by Support Element LIC.**

2069 **A set of activation profiles was changed. It was requested by Support Element(*{2}*) from *{0}.{1}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name

2070 **A set of activation profiles was changed. It was requested by Hardware Management Console(*{2}*) from *{0}.{1}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name

2071 **A set of activation profiles was changed. It was requested by Support Element(*{2}*) from *{0}.{1}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name
*{3}*Origin IP address

2072 **A set of activation profiles was changed. It was requested by Hardware Management Console(*{2}*) from *{0}.{1}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name
*{3}*Origin IP address

2073 **A set of activation profiles was imported.**

2074 **A set of activation profiles was imported. It was requested from *{0}.{1}*.**

Explanation

Substitution variables are:

*{1}*Network ID
*{2}*NAU

2075 **A set of activation profiles was imported. It was requested by *{2}* from *{0}.{1}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name

2076 **A set of activation profiles was imported. It was requested by *{2}* from *{0}.{1}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU

*{2}*User name
*{3}*Origin IP address

2077	**A set of activation profiles was imported. It was requested by Support Element LIC.**
2078	**A set of activation profiles was imported. It was requested by Support Element(*{2}*) from *{0}.{1}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name

2079	**A set of activation profiles was imported. It was requested by Hardware Management Console(*{2}*) from *{0}.{1}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name

2080	**A set of activation profiles was imported. It was requested by Support Element(*{2}*) from *{0}.{1}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name
*{3}*Origin IP address

2081	**A set of activation profiles was imported. It was requested by Hardware Management Console(*{2}*) from *{0}.{1}* at IP address *{3}*.**

Explanation

Substitution variables are:

*{0}*Network ID
*{1}*NAU
*{2}*User name
*{3}*Origin IP address

2082	**Concurrent internal code changes for PCIe Interconnect 2 started.**
2083	**Concurrent internal code changes for PCIe Interconnect 2 completed.**
2084	**Concurrent internal code changes for PCIe Interconnect 2 failed.**
2085	**Concurrent internal code changes for Power Distribution Units started.**
2086	**Concurrent internal code changes for Power Distribution Units completed.**
2087	**Concurrent internal code changes for Power Distribution Units failed.**
2088	**Concurrent internal code changes for Top of Rack Switch started.**

2089	**Concurrent internal code changes for Top of Rack Switch completed.**
2090	**Concurrent internal code changes for Top of Rack Switch failed.**
2091	**Concurrent internal code changes for BPA Controller started.**
2092	**Concurrent internal code changes for BPA Controller completed.**
2093	**Concurrent internal code changes for BPA Controller failed.**
2094	**Concurrent internal code changes for Cooling Unit Controller started.**
2095	**Concurrent internal code changes for Cooling Unit Controller completed.**
2096	**Concurrent internal code changes for Cooling Unit Controller failed.**
2097	**The following internal code changes were deleted because they are on hold: *{0}*.**

Explanation

Substitution variables are:

*{0}*Engineering change numbers

2098	**A load will be attempted for system *{0}*. The load type is NVMe load. Refer to the security log for more details.**

Explanation

Substitution variables are:

*{0}*Image name

2099	**A load will be attempted for system *{0}*. The load type is NVMe dump. Refer to the security log for more details.**

Explanation

Substitution variables are:

*{0}*Image name

2100	**Concurrent internal code changes for Service Infrastructure MCU started.**

Messages 2101-2200

2101	**Concurrent internal code changes for Service Infrastructure MCU completed.**
2102	**Concurrent internal code changes for Service Infrastructure MCU failed.**
2103	**Concurrent internal code changes for Container Firmware started.**
2104	**Concurrent internal code changes for Container Firmware completed.**
2105	**Concurrent internal code changes for Container Firmware failed.**
2106	**A new authorization code for Remote Code Load was created for *{0}* from *{1}* at *{2}*.**

Explanation

Substitution variables are:

*{0}*User id
*{1}*IP address
*{2}*Date

2107	**User *{0}* from *{1}* scheduled a Remote Code Load on *{2}* at *{3}***

Explanation

Substitution variables are:

*{0}*User id
*{1}*IP address
*{2}*Target id
*{3}*Date

2108 **User *{0}* from *{1}* cancelled a Remote Code Load on *{2}* at *{3}***

Explanation

Substitution variables are:

*{0}*User id
*{1}*IP address
*{2}*Target id
*{3}*Date

2109 **User *{0}* from *{1}* cancelled a Remote Code Load from a reschedule on *{2}* at *{3}*.**

Explanation

Substitution variables are:

*{0}*User id
*{1}*IP address
*{2}*Target id
*{3}*Date

Messages 3001-3100

3000 **Data Replication is assuming the role of PRIMARY**

3001 **Data Replication is assuming the role of REPLICA**

3002 **Data Replication is assuming the role of PEER**

3003 **Data Replication is DISABLED**

Messages 3201-3300

3263 **The *{0}* object was defined. Its serial number is *{1}*.**

Explanation

Substitution variables are:

*{0}*Object name
*{1}*Serial number

3264 **The *{0}* object was undefined. Its serial number was *{1}*.**

Explanation

Substitution variables are:

*{0}*Object name
*{1}*Serial number

3265 **Failed to copy *{0}* file from backup DVD into hard drive.**

Explanation

Substitution variables are:

*{0}*File name

3266 **Failed to extract file *{0}* from the ASN.1 formatted backup PK1 file.**

Explanation

Substitution variables are:

*{0}*File name

3267 **Failed to validate backup tar file *{0}*.**

Explanation

Substitution variables are:

*{0}*File name

3268 ***{0}* logs were removed.**

Explanation

Substitution variables are:

*{0}*Number of logs deleted

3269 ***{0}* logs were removed for the time period *{1}* UTC to *{2}* UTC.**

Explanation

Substitution variables are:

*{0}*Number of logs deleted
*{1}*Start time
*{2}*End time

Messages 3301-3400

3315 **The primary Support Element failed to send its backup file to the alternate Support Element.**

3316 **The primary Support Element successfully sent its backup file to the alternate Support Element.**

3317 **The backup file was created successfully. *{0}***

Explanation

Substitution variables are:

*{0}*The name and size of the backup file

3318 **SSLv3 protocol support has been *{0}* by *{1}* logged on from location *{2}*.**

Explanation

Substitution variables are:

*{0}*Enabled or disabled
*{1}*User name
*{2}*IP address and optional host name

3319 **RC4 cipher support has been *{0}* by *{1}* logged on from location *{2}*.**

Explanation

Substitution variables are:

*{0}*enabled or disabled
*{1}*User name; empty if unknown
*{2}*IP address and optional host name; empty if unknown

3320 **TLSv12 protocol support has been *{0}* by *{1}* logged on from location *{2}*.**

Explanation

Substitution variables are:

*{0}*Enabled or disabled
*{1}*User name
*{2}*IP address and optional host name

3321 **There is no alternate Support Element; therefore the primary Support Element backup file will remain only on the primary hard drive.**

3322 **The minimum TLS version has been set to *{0}* by *{1}* logged on from location *{2}*.**

Explanation

Substitution variables are:

*{0}*TLS protocol version
*{1}*User name
*{2}*IP address and optional host name

Messages 4001-4100

4051 **A device monitor event occurred; Device Type: *{0}*, Action: *{1}*, Vendor: *{2}*, Model: *{3}*, Serial: *{4}***

Explanation

Substitution variables are:

*{0}*Device type
*{1}*Event type
*{2}*Vendor name
*{3}*Device model number
*{4}*Device serial number

4061 **The following role(s) \n *{0}* \n have changed.**

Explanation

Substitution variables are:

*{0}*User role names

4100 **The service state for PDU side *{0}* has been enabled.**

Explanation

Substitution variables are:

*{0}*PDU side for which service state has been enabled.

Messages 4101-4200

4101 **The service state for PDU side *{0}* has been disabled**

Explanation

Substitution variables are:

*{0}*PDU side for which service state has been disabled.

4102 **Loose piece MES data restore was successful. Restore type is *{0}*.**

Explanation

Substitution variables are:

*{0}*Type of loose piece MES data

4103 **Loose piece MES data restore was unsuccessful. Restore type is *{0}*.**

Explanation

Substitution variables are:

*{0}*Type of loose piece MES data

Messages 5001-5100

5000 ***{0}* application opened.**

Explanation

Substitution variables are:

*{0}*Application name

5001 ***{0}* application closed.**

Explanation

Substitution variables are:

*{0}*Application name

5002 **Crypto adapter passphrase logon with profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Profile name

5003 **Crypto adapter group passphrase logon with profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Profile name

5004 **Crypto adapter group member passphrase logon with member *{0}*.**

Explanation

Substitution variables are:

*{0}*Member name

5005 **Crypto adapter smart card logon with profile *{0}*. Logon key ID: *{1}*. Card ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Profile name
*{1}*Key identifier
*{2}*Card identifier

5006 **Crypto adapter group smart card logon with profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Profile name

5007 **Crypto adapter group member smart card logon with member *{0}*. Logon key ID: *{1}***

Explanation

Substitution variables are:

*{0}*Member name
*{1}*Key identifier

5008 **Crypto adapter logoff for profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Profile name

5010 ***{0}* application failed to open. Return code *{1}*.**

Explanation

Substitution variables are:

*{0}*Application name
*{1}*Return code number

5011 ***{0}* application exited with return code *{1}*.**

Explanation

Substitution variables are:

*{0}*Application name
*{1}*Return code number

5012 **Crypto adapter passphrase logon failure with profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Profile name

5013 **Crypto adapter group passphrase logon failure with profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Profile name

5014 **Crypto adapter group member passphrase logon failed for member *{0}*.**

Explanation

Substitution variables are:

*{0}*Member name

5015 **Crypto adapter smart card logon failure with profile *{0}*. Card ID: *{1}*.**

Explanation

Substitution variables are:

*{0}*Profile name
*{1}*Card id number

5016 **Crypto Adapter Group Smart Card Logon Failure with Profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Profile name

5017 **Crypto Adapter Group Member Smart Card Logon Failed for Member *{0}*.**

Explanation

Substitution variables are:

*{0}*Member name

5018 **Crypto Adapter Logoff failed.**

5019 **Crypto Adapter Change Passphrase Failure with Profile *{0}*.**

Explanation

Substitution variables are:

*{0}*Profile name

5100 **Deleting Key *{0}* from TKE Workstation DES Key Storage.**

Explanation

Substitution variables are:

*{0}*Key name

Messages 5101-5200

5101 **Deleting Key *{0}* from TKE workstation PKA key storage. Key ID: *{1}***

Explanation

Substitution variables are:

*{0}*Key name
*{1}*Key identifier

5102 **Deleting Key *{0}* from TKE workstation AES key storage.**

Explanation

Substitution variables are:

*{0}*Key name

5110 **Delete Key *{0}* from TKE workstation DES key storage failed.**

Explanation

Substitution variables are:

*{0}*Key name

5111 **Delete Key *{0}* from TKE workstation PKA Key storage failed.**

Explanation

Substitution variables are:

*{0}*Key name

5112 **Delete Key *{0}* from TKE workstation AES Key storage failed.**

Explanation

Substitution variables are:

*{0}*Key name

5120 **A signature key was loaded. Authority index: *{0}*, Key ID: *{1}*.**

Explanation

Substitution variables are:

*{0}*Authority index number
*{1}*Key identifier

5121 **The signature key was unloaded. Authority index: *{0}*, Key ID: *{1}*.**

Explanation

Substitution variables are:

*{0}*Authority index number
*{1}*Key identifier

5122 **A *{0}* was deleted from a smart card. Card ID: *{1}*, Zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*Type of key deleted
*{1}*Card identifier

*{2}*Zone identifier

5123 **A *{0}* was copied to a smart card. Source card ID: *{1}*, Source zone ID: *{2}*, Target card ID: *{3}*, Target zone ID: *{4}***

Explanation

Substitution variables are:

*{0}*Type of key copied
*{1}*Source card identifier
*{2}*Source zone identifier
*{3}*Target card identifier
*{4}*Target zone identifier

5124 **A key part of type *{0}* was generated to print file *{2}* with description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Key type description
*{2}*File name

5125 **A key part of type *{0}* was generated to binary file *{2}* with description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Key type description
*{2}*File name

5126 **Generated signature key with index *{0}* to file *{1}* in *{2}*.**

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*File name
*{2}*Directory name

5127 **Generated signature key with index *{0}* to TKE workstation PKA key storage.**

Explanation

Substitution variables are:

*{0}*Authority index

5128 **Generated signature key with index *{0}* to smart card. Card ID: *{1}*, Zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Card identifier
*{2}*Zone identifier

5129 **Deleted authority signature key with index *{0}* on smart card. Card ID: *{1}*, Zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Card identifier
*{2}*Zone identifier

5130 **Generated RSA key to file *{0}*, Key ID: *{1}***

Explanation

Substitution variables are:

*{0}*File name
*{1}*Key identifier

5131 **RSA key was loaded to the host. Key ID: *{0}* Loaded to location: *{1}***

Explanation

Substitution variables are:

*{0}*Key identifier
*{1}*Dataset

5132 **Enciphered RSA key to file *{0}*, Key ID: *{1}***

Explanation

Substitution variables are:

*{0}*File name
*{1}*Key identifier

5133 **Generated an administrator signature key on a smart card. Name: *{0}*, SKI: *{1}*, Card ID: *{2}*, Zone ID: *{3}***

Explanation

Substitution variables are:

*{0}*Authority name
*{1}*Subject key identifier
*{2}*Card idendifier
*{3}*Zone identifier

5134 **Deleted an administrator signature key from a smart card. Name: *{0}*, SKI: *{1}*, Card ID: *{2}*, Zone ID: *{3}***

Explanation

Substitution variables are:

*{0}*Authority name
*{1}*Subject key identifier
*{2}*Card identifier
*{3}*Zone idenditier

5135 **A binary file key part was copied to a smart card. Source binary file: *{0}*, Target card ID: *{1}*, Target zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*File name
*{1}*Target card identifier
*{2}*Target zone identifier

5150 **Failure loading a signature key. Authority index: *{0}*, Key ID: *{1}*.**

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Key identifier

5151 **Failure during smart card delete. Card ID: *{0}*, Zone ID: *{1}***

Explanation

Substitution variables are:

*{0}*Card identifier
*{1}*Zone identifier

5152 **Failure during smart card copy. Source card ID: *{0}*, Source zone ID: *{1}*, Target card ID: *{2}*, Target zone ID: *{3}***

Explanation

Substitution variables are:

*{0}*Source card identifier
*{1}*Source zone identifier
*{2}*Target card identifier
*{3}*Target zone identifier

5153 **A key part of type *{0}* failed generation to print file *{2}* with description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Key description
*{2}*File name

5154 **A key part of type *{0}* failed generation to binary file *{2}* with description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Key description
*{2}*File name

5155 **Failed to generate authority signature key with index *{0}* to file.**

Explanation

Substitution variables are:

*{0}*Authority index

5156 **Failed to generate authority signature key with index *{0}* to TKE workstation PKA key storage.**

Explanation

Substitution variables are:

*{0}*Authority index

5157 **Failed to generate authority signature key with index *{0}* to smart card. Card ID: *{1}*, Zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Card identifier
*{2}*Zone identifier

5158 **Failed to delete authority signature key with index *{0}* on smart card. Card ID: *{1}*, Zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Card identifier
*{2}*Zone identifier

5159 **Failed to generate RSA key to file.**

5160 **Load of RSA key failed.**

5161 **Encipher of RSA key failed.**

5162 **Failure generating an administrator signature key on a smart card. Card ID: *{0}*, Zone ID: *{1}*, Failure details: *{2}***

Explanation

Substitution variables are:

*{0}*Card identifier
*{1}*Zone identifier
*{2}*Failure details

5163 **Failure deleting an administrator signature key from a smart card. Card ID: *{0}*, Zone ID: *{1}*, Failure details: *{2}***

Explanation

Substitution variables are:

*{0}*Card identifier
*{1}*Zone identifier
*{2}*Failure details

5164 **Failure during binary file to smart card copy. Source binary file: *{0}*, Target card ID: *{1}*, Target zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*File name
*{1}*Target card identifier
*{2}*Target zone identifier

5200 **A valid PIN was entered for *{0}* in *{1}*. Card ID: *{2}*, Zone ID: *{3}***

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Card reader description
*{2}*Card identifier
*{3}*Zone idendifier

Messages 5201-5300

5201 **A key part was generated on smart card in reader *{0}*. Card ID: *{1}*, Zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*Reader number
*{1}*Card identifier
*{2}*Zone identifier

5202 **Secure key entry to smart card in *{0}* completed. Card ID: *{1}*, Zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*Reader number
*{1}*Card identifier
*{2}*Zone identifier

5250 **Failure during PIN entry for *{0}* in *{1}*. Card ID: *{2}*, Zone ID: *{3}***

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Card reader description
*{2}*Card identifier
*{3}*Zone identifier

5251 **Tried to access a *{0}* with a blocked PIN. Card ID: *{1}*, Zone ID: *{2}*, Operation: *{3}*.**

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Card identifier
*{2}*Zone identifier
*{3}*Operation

5252 **Tried to access a *{0}* not in the same zone as the TKE crypto adapter. Card ID: *{1}*, Card Zone ID: *{2}*, TKE crypto adapter zone ID: *{3}*, Operation: *{4}***

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Card identifier
*{2}*Card zone identifier
*{3}*Crypto adapter zone identifier
*{4}*Operation

5253 **Failure during key part generation using reader *{0}*. Card ID: *{1}*, Zone ID: *{2}*, Key type: *{3}*, Key description: *{4}***

Explanation

Substitution variables are:

*{0}*Reader number
*{1}*Card identifier
*{2}*Zone identifier
*{3}*Key type
*{4}*Key description

5254 **Secure key entry failed to smart card in *{0}*. Card ID: *{1}*, Zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*Card reader description
*{1}*Card identifier
*{2}*Zone identifier

5300 **The crypto module description has been updated to *{0}*.**

Explanation

Substitution variables are:

*{0}*New description

Messages 5301-5400

5301 **Released crypto module.**

5302 **Forced release of crypto module.**

5303 **Reserved crypto module.**

5304 **Load role issued to create a module-wide role. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Role description

5305 **Load role issued to change a module-wide role. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Role description

5306 **Delete module-wide role issued. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Role description

5307 **Load authority issued to create a module-wide authority. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telephone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Authority index
*{2}*Role identifier
*{3}*Telephone number
*{4}*Email address
*{5}*Address
*{6}*Authority description
*{7}*Tower serial number
*{8}*Key identifier

5308 **Load authority issued to change a module-wide authority. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telephone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Authority index
*{2}*Role identifier
*{3}*Telephone number
*{4}*Email address
*{5}*Address
*{6}*Authority description
*{7}*Tower serial number
*{8}*Key identifier

5309 **Delete module-wide authority issued. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telephone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Authority index
*{2}*Role identifier
*{3}*Telephone number
*{4}*Email address
*{5}*Address
*{6}*Authority description
*{7}*Tower serial number
*{8}*Key identifier

5310 **Host user ID *{0}* logged onto host *{1}* with mixed case password support set to *{2}*.**

Explanation

Substitution variables are:

*{0}*User identifier
*{1}*Host name
*{2}*Mixed case choice

5311 **Logoff host *{0}***

Explanation

Substitution variables are:

*{0}*Host name

5312 **Host *{0}* opened.**

Explanation

Substitution variables are:

*{0}*Host name

5313 **Host user ID *{0}* logged onto group *{1}* with mixed case password support set to *{2}*.**

Explanation

Substitution variables are:

*{0}*User identifier
*{1}*Group name
*{2}*Mixed case choice

5314 **Group *{0}* opened.**

Explanation

Substitution variables are:

*{0}*Group name

5315 **Host Query for environment settings, Time = *{0}*, ICSF FMID = *{1}*, Date = *{2}*, Access control = *{3}*.**

Explanation

Substitution variables are:

*{0}*Time
*{1}*Function modification identifier
*{2}*Date
*{3}*Host access control

5316 **A key part of type *{0}* was loaded to key part register labeled *{1}* in domain *{2}*.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Key label
*{2}*Domain index

5317 **A key part of type *{0}* with description *{1}* and label *{2}* was loaded to TKE workstation key storage.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Key description
*{2}*Key label

5318 **Key part register labeled *{0}* completed for domain *{1}*.**

Explanation

Substitution variables are:

*{0}*Key label
*{1}*Domain index

5319 **Operational key part register *{0}* was cleared for for domain *{1}*.**

Explanation

Substitution variables are:

*{0}*Key label
*{1}*Domain index

5320 ***{0}* Register in domain *{1}* was cleared.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Domain index

5321 **Crypto module in index *{0}* was disabled by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Crypto module index
*{1}*Authority index
*{2}*Key identifier

5322 **Command enable crypto module for crypto module in index *{0}* was issued.**

Explanation

Substitution variables are:

*{0}*Crypto module index

5323 **Command enable crypto module for crypto module in index *{0}* was cosigned by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Crypto module index
*{1}*Authority index
*{2}*Key identifier

5324 **Zeroize issued for domain index *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5325 **Zeroize cosigned for domain index *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier

5326 **Changed signature key index from *{0}* to *{1}*.**

Explanation

Substitution variables are:

*{0}*Old index
*{1}*New index

5327 **Load role issued to update domain controls for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5328 **Pending command *{2}* deleted by authority index *{1}* on host crypto module index *{0}*, TSN: *{3}*, Signature key ID: *{4}***

Explanation

Substitution variables are:

*{0}*Crypto module index
*{1}*Authority index
*{2}*Command
*{3}*Tower serial number
*{4}*Key identifier

5329 **Pending command *{2}* cosigned by authority index *{1}* on host crypto module index *{0}*, TSN: *{3}*, Signature key ID: *{4}***

Explanation

Substitution variables are:

*{0}*Crypto module index
*{1}*Authority index
*{2}*Command
*{3}*Tower serial number
*{4}*Key identifier

5330 **Crypto module with ID *{0}* was authenticated and *{1}* by the user.**

Explanation

Substitution variables are:

*{0}*Crypto module identifier
*{1}*Authentication result

5331 **The *{0}* Register in domain *{1}* was loaded. *{2}* Key part hash: *{3}***

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Domain index
*{2}*Key part loaded
*{3}*Key part hash

5332 **The *{0}* Register for domain *{1}* was set.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Domain index

5333 **Not authorized to verb *{0}* on TKE workstation crypto adapter.**

Explanation

Substitution variables are:

*{0}*Verb name

5334 **Configuration information from file *{0}* was applied to the crypto module at index *{1}* on host *{2}*. *{3}***

Explanation

Substitution variables are:

*{0}*File name
*{1}*Crypto module index
*{2}*Host identifier
*{3}*Audit text

5335 **Configuration information was collected from the crypto module at index *{0}* on host *{1}* and saved in the file *{2}*.**

Explanation

Substitution variables are:

*{0}*Crypto module index
*{1}*Host identifier
*{2}*File name

5336 **The crypto module at index *{0}* on host *{1}* was enrolled in migration zone *{2}*.**

Explanation

Substitution variables are:

*{0}*Crypto module index
*{1}*Host identifier
*{2}*Zone identifier

5337 **An IA smart card has approved applying configuration data to a target crypto module or domain group. Card ID: *{0}*, Zone ID: *{1}***

Explanation

Substitution variables are:

*{0}*Card identifier
*{1}*Zone identifier

5338 **A KPH smart card has approved rewrapping the transport key during configuration migration. Card ID: *{0}*, Zone ID: *{1}***

Explanation

Substitution variables are:

*{0}*Card identifier
*{1}*Zone identifier

5339 **The default key wrapping method for *{0}* was changed to *{1}* for domain *{2}*.**

Explanation

Substitution variables are:

*{0}*Token type
*{1}*Wrapping method
*{2}*Domain index

5340 **Decimalization tables were activated in domain *{0}* using authority index *{1}*. Signature key ID: *{2}*. Tables activated:**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier

5341 **Decimalization tables were deleted in domain *{0}* using authority index *{1}*. Signature key ID: *{2}*. Tables deleted: *{3}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier
*{3}*Deleted table list

5342 **Decimalization tables were loaded in domain *{0}* using authority index *{1}*. Signature key ID: *{2}*. Tables loaded: *{3}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier
*{3}*Loaded table list

5343 **Restricted PINs were activated in domain *{0}* using authority index *{1}*. Signature key ID: *{2}*. PINs activated: *{3}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier
*{3}*Activated pins list

5344 **Restricted PINs were deleted in domain *{0}* using authority index *{1}*. Signature key ID: *{2}*. PINs deleted: *{3}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier
*{3}*Deleted pins list

5345 **Restricted PIN loaded in domain *{0}* using authority index *{1}*. Signature key ID: *{2}*. PIN loaded: *{3}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier
*{3}*Loaded pins list

5346 **Data set *{0}* on host *{1}* was allocated successfully.**

Explanation

Substitution variables are:

*{0}*Data set name
*{1}*Host name

5347 **Coordinated change master key for data set type *{0}* domain *{1}* crypto module *{2}* host *{3}* was successful.**

Explanation

Substitution variables are:

*{0}*Data set type
*{1}*Domain index
*{2}*Crypto module index
*{3}*Host name

5348 **Access control tracking *{0}* request was issued for domain *{1}*.**

Explanation

Substitution variables are:

*{0}*Request type
*{1}*Domain index

5349 **The clock on the crypto module on host *{0}* at index *{1}* was set to *{2}*.**

Explanation

Substitution variables are:

*{0}*Host
*{1}*Crypto module index
*{2}*New time

5350 **Certificate with label *{0}* was activated in domain *{1}* using authority index *{2}*, signature key ID: *{3}*.**

Explanation

Substitution variables are:

*{0}*Label name
*{1}*Domain index
*{2}*Authority index
*{3}*Signature key identifier

5351 **Certificate label changed from *{0}* to *{1}* in domain *{2}* using authority index *{3}*, signature key ID: *{4}*.**

Explanation

Substitution variables are:

*{0}*Old label name
*{1}*New label name
*{2}*Domain index
*{3}*Authority index
*{4}*Signature key identifier

5352 **Deleted certificate *{0}* from domain *{1}* using authority index *{2}*, signature key ID: *{3}*.**

Explanation

Substitution variables are:

*{0}*Certificate name
*{1}*Domain index
*{2}*Authority index
*{3}*Signature key identifier

5353 **Certificate with label *{0}* was loaded in domain *{1}* using authority index *{2}*, signature key ID: *{3}*.**

Explanation

Substitution variables are:

*{0}*Certificate name
*{1}*Domain index
*{2}*Authority index
*{3}*Signature key identifier

5354 **Certificate with label *{0}* was replaced in domain *{1}* using authority index *{2}*, signature key ID: *{3}*.**

Explanation

Substitution variables are:

*{0}*Certificate name
*{1}*Domain index
*{2}*Authority index
*{3}*Signature key identifier

5355 **Load role issued to create a domain-specific role for domain *{2}*. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Description
*{2}*Domain inde

5356 **Load role issued to change a domain-specific role for domain *{2}*. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Description
*{2}*Domain index

5357 **Delete domain-specific role issued for domain *{2}*. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Description
*{2}*Domain index

5358 **Load authority issued to create a domain-specific authority for domain *{9}*. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telephone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Index
*{2}*Role identifier
*{3}*Telephone number
*{4}*Email
*{5}*Address
*{6}*Authority description
*{7}*TSN
*{8}*Authority signature key identifier
*{9}*Domain index

5359 **Load authority issued to change a domain-specific authority for domain *{9}*. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telephone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Index
*{2}*Role identifier
*{3}*Telephone number
*{4}*Email
*{5}*Address
*{6}*Authority description
*{7}*TSN
*{8}*Authority signature key identifier
*{9}*Domain index

5360 **Delete domain-specific authority issued for domain *{9}*. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telephone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Index
*{2}*Role identifier
*{3}*Telphone number
*{4}*Email
*{5}*Address
*{6}*Authority description
*{7}*TSN
*{8}*Authority signature key identifier
*{9}*Domain index

5361 **Enter imprint mode issued for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5362 **Enter imprint mode cosigned for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5363 **Enter PCI-compliant mode issued for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5364 **Enter PCI-compliant mode cosigned for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5365 **Exit PCI-compliant mode issued for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5366 **Exit PCI-compliant mode cosigned for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5367 **Enter migration mode issued for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5368 **Enter migration mode cosigned for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5369 **Exit migration mode issued for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5370 **Exit migration mode cosigned for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5371 **Migration mode was extended 24 hours for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5372 **Clear secure audit log issued for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5373 **Clear secure audit log cosigned for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5374 **Load role cosigned to create a module-wide role by authority index *{0}*, Signature key ID: *{1}*.**

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Signature key identifier

5375 **Load role cosigned to change a module-wide role by authority index *{0}*, Signature key ID: *{1}*.**

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Signature key identifier

5376 **Delete module-wide role cosigned by authority index *{0}*, Signature key ID: *{1}*.**

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Signature key identifier

5377 **Load authority cosigned to create a module-wide authority by authority index *{0}*, Signature key ID: *{1}*.**

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Signature key identifier

5378 **Load authority cosigned to change a module-wide authority by authority index *{0}*, Signature key ID: *{1}*.**

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Signature key identifier

5379 **Delete module-wide authority cosigned by authority index *{0}*, Signature key ID: *{1}*.**

Explanation

Substitution variables are:

*{0}*Authority index
*{1}*Signature key identifier

5380 **Load role cosigned to create a domain-specific role for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5381 **Load role cosigned to change a domain-specific role for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5382 **Delete domain-specific role cosigned for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5383 **Load authority cosigned to create a domain-specific authority for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5384 **Load authority cosigned to change a domain-specific authority for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5385 **Delete domain-specific authority cosigned for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5386 **Load role cosigned to update domain controls for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Signature key identifier

5387 **Exit imprint mode completed for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5400 **A Crypto module description update failed for description: *{0}*.**

Explanation

Substitution variables are:

*{0}*Description

Messages 5401-5500

5401 **Failed to release crypto module.**

5402 **Failed to force release of crypto module reserved by *{0}*.**

Explanation

Substitution variables are:

*{0}*Reserver

5403 **Failed to reserve crypto module.**

5404 **Failure issuing Load role to create a module-wide role. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier

*{1}*Description

5405 **Failure issuing Load role to change a module-wide role. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Description

5406 **Failure issuing Delete module-wide role. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Description

5407 **Failure issuing Load authority to create a module-wide authority. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telephone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Index
*{2}*Role identifier
*{3}*Telephone number
*{4}*Email
*{5}*Address
*{6}*Authority description
*{7}*Tower serial number
*{8}*Key identifier

5408 **Failure issuing Load authority to change a module-wide authority. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telphone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Index
*{2}*Role identifier
*{3}*Telephone number
*{4}*Email
*{5}*Address
*{6}*Authority description
*{7}*Tower serial number
*{8}*Key identifier

5409 **Failure issuing Delete module-wide authority. Index: *{1}*, name: *{0}*, Role ID: *{2}*, Telephone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Index
*{2}*Role identifier
*{3}*Telephone number
*{4}*Email
*{5}*Address
*{6}*Authority description
*{7}*Tower serial number
*{8}*Key identifier

5410 **User *{0}* logon failed for host *{1}* with mixed case password support set to *{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Host name
*{2}*Mixed case setting

5411 **Host *{0}* failed to open.**

Explanation

Substitution variables are:

*{0}*Host name

5412 **User *{0}* logon failed for group *{1}* with mixed case password support set to *{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Group name
*{2}*Mixed case setting

5413 **Group *{0}* failed to open.**

Explanation

Substitution variables are:

*{0}*Group name

5414 **Host Query for environment settings failed, Time = *{0}*, ICSF FMID = *{1}*, Date = *{2}*, Access control = *{3}*.**

Explanation

Substitution variables are:

*{0}*Time
*{1}*Function modification identifier
*{2}*Date
*{3}*Access control

5415 **A key part of type *{0}* with description *{1}* failed to load to key part register labeled *{2}*.**

Explanation

Substitution variables are:

*{0}*Key part type
*{1}*Key part description
*{2}*Key part label

5416 **A key part of type *{0}* with description *{1}* and label *{2}* failed to load into TKE workstation key storage.**

Explanation

Substitution variables are:

*{0}*Key part type
*{1}*Key part description
*{2}*Key part label

5417 **Key part register labeled *{0}* failed completion.**

Explanation

Substitution variables are:

*{0}*Key label

5418 **Operational key part register labeled *{0}* failed to be cleared.**

Explanation

Substitution variables are:

*{0}*Key label

5419 **Failed to clear *{0}* Register in domain *{1}*.**

Explanation

Substitution variables are:

*{0}*Key label
*{1}*Domain index

5420 **Crypto module in index *{0}* failed to be disabled by authority index *{1}*, signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Crypto module index
*{1}*Authority index
*{2}*Key identifier

5421 **Failure issuing enable of crypto module in index *{0}*.**

Explanation

Substitution variables are:

*{0}*Crypto module index

5422 **Failure cosigning enable of crypto module in index *{0}*.**

Explanation

Substitution variables are:

*{0}*Crypto module index

5423 **Failure issuing zeroize of domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5424 **Failure issuing Load role to update domain controls for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5425 **Pending command *{2}* deletion failure by authority index *{1}* on host crypto module index *{0}*, TSN: *{3}*, Signature key ID: *{4}***

Explanation

Substitution variables are:

*{0}*Crypto module index
*{1}*Authority index
*{2}*Command type
*{3}*Tower serial number
*{4}*Key identifier

5426 **Pending command *{2}* cosign failure by authority index *{1}* on host crypto module index *{0}*, TSN: *{3}*, Signature key ID: *{4}***

Explanation

Substitution variables are:

*{0}*Crypto module index
*{1}*Authority index
*{2}*Command type
*{3}*Tower serial number
*{4}*Key identifier

5427 **Crypto module authentication failure for crypto module with ID *{0}*.**

Explanation

Substitution variables are:

*{0}*Crypto module identifier

5428 **Failure loading the *{0}* Register in domain *{1}*. *{2}***

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Domain index
*{2}*Key part

5429 **Failure setting the *{0}* Register for domain *{1}*.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Domain index

5430 **Error in *{0}* task of configuration migration utility: *{1}***

Explanation

Substitution variables are:

*{0}*Task name
*{1}*Error reason

5431 **Error in collect task of configuration migration utility: *{0}***

Explanation

Substitution variables are:

*{0}*Error reason

5432 **Error in enroll task of configuration migration utility: *{0}***

Explanation

Substitution variables are:

*{0}*Error reason

5433 **IA smart card approval failed during apply task of configuration migration.**

5434 **KPH smart card approval failed during apply task of configuration migration.**

5435 **Error occurred when changing the default key wrapping method for *{0}* to *{1}* for domain *{2}*.**

Explanation

Substitution variables are:

*{0}*Token type
*{1}*Wrapping method
*{2}*Domain index

5436 **Activate decimalization tables failed for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier

5437 **Delete decimalization tables failed for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier

5438 **Load decimalization tables failed for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier

5439 **Activate restricted PINs failed for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier

5440 **Delete restricted PINs failed for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier

5441 **Load restricted PINs failed for domain *{0}* by authority index *{1}*, Signature key ID: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Authority index
*{2}*Key identifier

5442 **Data set *{0}* on host *{1}* allocation failed.**

Explanation

Substitution variables are:

*{0}*Data set name
*{1}*Host name

5443 **Coordinated change master key for data set type *{0}* domain *{1}* crypto module *{2}* host *{3}* failed.**

Explanation

Substitution variables are:

*{0}*Data set type
*{1}*Domain index
*{2}*Crypto module index
*{3}*Host name

5444 **Access control tracking *{0}* request failed for domain *{1}* by authority index *{2}* Signature key ID *{3}*.**

Explanation

Substitution variables are:

*{0}*Request type
*{1}*Domain index
*{2}*Authority index
*{3}*Key identifier

5445 **Failure setting the clock on the crypto module on host *{0}* at index *{1}*.**

Explanation

Substitution variables are:

*{0}*Host Name
*{1}*Crypto module index

5446 **Certificate with label *{0}* activate request failed for domain *{1}* by authority index *{2}*, Signature key ID *{3}*.**

Explanation

Substitution variables are:

*{0}*Certificate label name
*{1}*Domain index
*{2}*Authority index
*{3}*Signature key identifier

5447 **Failed request to change certificate label from *{0}* to *{1}* for domain *{2}* by authority index *{3}*, Signature key ID *{4}*.**

Explanation

Substitution variables are:

*{0}*Old certificate label name
*{1}*New certificate label name
*{2}*Domain index
*{3}*Authority index
*{4}*Signature key identifier

5448 **Failed request to delete certificate *{0}* for domain *{1}* by authority index *{2}*, Signature key ID *{3}*.**

Explanation

Substitution variables are:

*{0}*Certificate name
*{1}*Domain index
*{2}*Authority index
*{3}*Signature key identifier

5449 **Failed request to load certificate *{0}* for domain *{1}* by authority index *{2}*, Signature key ID *{3}*.**

Explanation

Substitution variables are:

*{0}*Certificate name
*{1}*Domain index
*{2}*Authority index
*{3}*Signature key identifier

5450 **Failed request to replace certificate *{0}* for domain *{1}* by authority index *{2}*, Signature key ID *{3}*.**

Explanation

Substitution variables are:

*{0}*Certificate name
*{1}*Domain index
*{2}*Authority index
*{3}*Signature key identifier

5451 **Failure issuing load role to create a domain-specific role for domain *{2}*. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Description
*{2}*Domain index

5452 **Failure issuing load role to change a domain-specific role for domain *{2}*. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Description
*{2}*Domain index

5453 **Failure issuing Delete domain-specific role for domain *{2}*. Role ID: *{0}*, description: *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*Description
*{2}*Domain index

5454 **Failure issuing Load authority to create a domain-specific authority for domain *{9}*. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telephone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Index
*{2}*Role identifier
*{3}*Telephone number
*{4}*Email
*{5}*Address
*{6}*Authority description
*{7}*TSN
*{8}*Authority signature key identifier
*{9}*Domain index

5455 **Failure issuing Load authority to change a domain-specific authority for domain *{9}*. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telphone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Index
*{2}*Role identifier
*{3}*Telephone number
*{4}*Email
*{5}*Address
*{6}*Authority description
*{7}*TSN
*{8}*Authority signature key identifier
*{9}*Domain index

5456 **Failure issuing Delete domain-specific authority for domain *{9}*. Index: *{1}*, Name: *{0}*, Role ID: *{2}*, Telephone: *{3}*, Email: *{4}*, Address: *{5}*, Authority description: *{6}*, TSN: *{7}*, Authority signature key ID: *{8}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Index
*{2}*Role identifier
*{3}*Telphone number
*{4}*Email
*{5}*Address
*{6}*Authority description
*{7}*TSN
*{8}*Authority signature key identifier
*{9}*Domain index

5457 **Failure cosigning load role to create a domain-specific role for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5458 **Failure cosigning load role to change a domain-specific role for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5459 **Failure cosigning delete domain-specific role for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5460 **Failure cosigning load authority to create a domain-specific authority for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5461 **Failure cosigning load authority to change a domain-specific authority for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5462 **Failure cosigning Delete domain-specific authority for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5463	**Failure cosigning load role to create a module-wide role.**
5464	**Failure cosigning load role to change a module-wide role.**
5465	**Failure cosigning Delete module-wide role.**
5466	**Failure cosigning load authority to create a module-wide authority.**
5467	**Failure cosigning Load authority to change a module-wide authority.**
5468	**Failure cosigning delete module-wide authority.**
5469	**Failure cosigning zeroize of domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5470	**Failure cosigning load role to update domain controls for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5471	**Failure issuing enter imprint mode for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5472	**Failure cosigning enter imprint mode for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5473	**Failure issuing enter PCI-compliant mode for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5474	**Failure cosigning enter PCI-compliant mode for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5475	**Failure issuing exit PCI-compliant mode for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5476 Failure cosigning exit PCI-compliant mode for domain *{0}*.

Explanation

Substitution variables are:

*{0}*Domain index

5477 Failure issuing enter migration mode for domain *{0}*.

Explanation

Substitution variables are:

*{0}*Domain index

5478 Failure cosigning enter migration mode for domain *{0}*.

Explanation

Substitution variables are:

*{0}*Domain index

5479 Failure issuing exit migration mode for domain *{0}*.

Explanation

Substitution variables are:

*{0}*Domain index

5480 Failure cosigning exit migration mode for domain *{0}*.

Explanation

Substitution variables are:

*{0}*Domain index

5481 Failure extending migration mode for domain *{0}*.

Explanation

Substitution variables are:

*{0}*Domain index

5482 Failure issuing clear secure audit log for domain *{0}*.

Explanation

Substitution variables are:

*{0}*Domain index

5483 Failure cosigning clear secure audit log for domain *{0}*.

Explanation

Substitution variables are:

*{0}*Domain index

5484 Failure exiting imprint mode for domain *{0}*.

Explanation

Substitution variables are:

*{0}*Domain index

5500 **Added a crypto module administrator. Name: *{0}*, SKI: *{1}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Subject key identifier

Messages 5501-5600

5501 **Added an administrator to domain *{0}*. Name: *{1}*, SKI: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*name
*{2}*Subject key identifier

5502 **Cleared the current master key in domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5503 **Cleared the new master key in domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5504 **The new master key in domain *{0}* was committed. Verification pattern: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Verification pattern

5505 **A master key in domain *{0}* was set to a random value. Verification pattern: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Verification pattern

5506 **The crypto module at index *{0}* was disabled.**

Explanation

Substitution variables are:

*{0}*Crypto module index

5507 **The crypto module at index *{0}* was enabled.**

Explanation

Substitution variables are:

*{0}*Crypto module index

5508 **An importer key pair was generated for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5509 **An invalid signature key was provided for a command. Command target: *{0}*, Name: *{1}*, SKI: *{2}*.**

Explanation

Substitution variables are:

*{0}*Command target
*{1}*Name
*{2}*Subject key identifier

5510 **The new master key in domain *{0}* was loaded. Number of parts: *{1}*, Final verification pattern: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Number of parts
*{2}*Verification pattern

5511 **Removed a crypto module administrator. Name: *{0}*, SKI: *{1}*.**

Explanation

Substitution variables are:

*{0}*Name
*{1}*Subject key identifier

5512 **Removed an administrator from domain *{0}*. Name: *{1}*, SKI: *{2}*.**

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Name
*{2}*Subject key identifier

5513 **The EP11 Master Key Register for domain *{0}* was set. Verification pattern: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Verification pattern

5514 **Updated the crypto module attributes.**

5515 **Updated the attributes for domain *{0}*.**

Explanation

Substitution variables are:

*{0}*Domain index

5516 **The control points for domain *{0}* were updated.**

Explanation

Substitution variables are:

*{0}*Domain index

5517 **The crypto module at index *{0}* was zeroized.**

Explanation

Substitution variables are:

*{0}*Domain index

5518 **Domain *{0}* was zeroized.**

Explanation

Substitution variables are:

*{0}*Domain index

5550 **Failure adding a crypto module administator. Name: *{0}*, SKI: *{1}*, Failure details: *{2}***

Explanation

Substitution variables are:

*{0}*Name
*{1}*Subject key identifier
*{2}*Failure details

5551 **Failure adding an administrator to domain *{0}*. Name: *{1}*, SKI: *{2}*, Failure details: *{3}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Name
*{2}*Subject key identifier
*{3}*Failure details

5552 **Failure clearing the current master key in domain *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5553 **Failure clearing the new master key in domain *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5554 **Failure committing the new master key in domain *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5555 **Failure setting a master key in domain *{0}* to a random value. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5556 **Failure disabling the crypto module at index *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5557 **Failure enabling the crypto module at index *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5558 **Failure generating an importer key pair for domain *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5559 **Failure loading new master key in domain *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5560 **Failure removing a crypto module administrator. Name: *{0}*, SKI: *{1}*, Failure details: *{2}***

Explanation

Substitution variables are:

*{0}*Name
*{1}*Subject key identifier
*{2}*Failure details

5561 **Failure removing an administrator from domain *{0}*. Name: *{1}*, SKI: *{2}*, Failure details: *{3}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Name
*{2}*Subject key identifier
*{3}*Failure details

5562 **Failure setting the EP11 master key register for domain *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5563 **Failure updating the crypto module attributes. Failure details: *{0}***

Explanation

Substitution variables are:

*{0}*Failure details

5564 **Failure updating the attributes for domain *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5565 **Failure updating the control points for domain *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index

*{1}*Failure details

5566 **Failure zeroizing the crypto module at index *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Crypto module index
*{1}*Failure details

5567 **Failure zeroizing domain *{0}*. Failure details: *{1}***

Explanation

Substitution variables are:

*{0}*Domain index
*{1}*Failure details

5600 **DH Transport key policy set to: Always use current transport key.**

Messages 5601-5700

5601 **DH Transport key policy set to: Always establish new transport key based on current values of Diffie-Hellman modulus and generator.**

5602 **DH Transport key policy set to: Always generate new values of Diffie-Hellman modulus and generator and establish new transport key.**

5603 **Change protocol parameters button was selected. Current DH values have been cleared. New values will be generated when needed.**

5604 **New Diffie-Hellman transport key was generated.**

5605 **New Diffie-Hellman modulus and generator values were generated.**

5610 **DH Transport key policy setting failed: Always use current transport key.**

5611 **DH Transport key policy setting failed: Always establish new transport key based on current values of Diffie-Hellman modulus and generator.**

5612 **DH Transport key policy setting failed: Always generate new values of Diffie-Hellman modulus and generator and establish new transport key.**

5613 **Change protocol parameters button failed selection.**

5614 **New Diffie-Hellman transport key failed generation.**

5615 **New Diffie-Hellman modulus and generator values failed generation.**

5620 **ECDH Transport key policy set to: Always use current transport key.**

5621 **ECDH Transport key policy set to: Always establish new transport key.**

5622 **Change protocol parameters button was selected. Current ECDH parameters have been cleared. New parameters will be used when needed.**

5623 **New ECDH transport key was generated.**

5624 **New ECDH parameters were used.**

5630 **ECDH transport key policy setting failed: Always use current transport key.**

5631 **ECDH transport key policy setting failed: Always establish new transport key.**

5632 **Change protocol parameters button failed selection.**

5633 **New ECDH transport key failed generation.**

5634	**Use new ECDH parameters failed.**
5640	**The CCA CLU utility was opened.**
5641	**The CCA CLU utility was closed.**
5642	**The following CLU command was executed: *{0}***

Explanation

Substitution variables are:

*{0}*Command

5643	**The following CLU command failed during execution: *{0}***

Explanation

Substitution variables are:

*{0}*Command

5644	**The CCA CLU utility output log was cleared.**
5645	**The CCA CLU utility output log clear function failed.**
5646	**The CCA CLU utility command history was cleared.**
5647	**The CCA CLU utility command history clear function failed.**
5650	**Cryptographic node management batch initializer executing script from *{0}*.**

Explanation

Substitution variables are:

*{0}*File name

5651	**Cryptographic node management batch initializer job output.**
5652	**The Cryptographic node management batch initializer failed to execute successfully.**
5653	**A Failure occurred displaying cryptographic node management batch initializer output.**
5660	**CCA node management utility - Started *{0}* smart cards supported**

Explanation

Substitution variables are:

*{0}*Smart cards supported setting

5661	**CCA node management utility - Exited**
5662	**CCA node management utility exit failure.**
5670	**Workstation crypto adapter authorizations loaded from *{0}*.**

Explanation

Substitution variables are:

*{0}*File name

5671	**Workstation crypto adapter authorization load failure.**
5672	**Workstation crypto adapter existing authorizations cleared.**
5673	**Workstation crypto adapter authorization clear failure.**

5674	**Workstation crypto adapter intrusion latch was reset.**
5675	**Workstation crypto adapter intrusion latch reset failure.**
5676	**Time on workstation crypto adapter synchronized with workstation clock.**
5677	**Workstation crypto adapter time synchronization failure.**
5678	**Workstation crypto adapter was initialized.**
5679	**Workstation crypto adapter initialization failure.**
5680	**Environment ID *{0}* set on the workstation crypto adapter.**

Explanation

Substitution variables are:

*{0}*Environmental identifier

5681	**Workstation crypto adapter environment ID set failure.**
5690	**DES KEK key part *{0}* was opened from *{1}*.**

Explanation

Substitution variables are:

*{0}*Key label
*{1}*File name

5691	**Failure occurred accessing DES KEK key part from *{0}*.**

Explanation

Substitution variables are:

*{0}*File name

5692	**DES KEK key part *{0}* was saved to *{1}*.**

Explanation

Substitution variables are:

*{0}*Key label
*{1}*File name

5693	**Failure occurred saving DES KEK key part *{0}* to *{1}*.**

Explanation

Substitution variables are:

*{0}*Key label
*{1}*File name

5694	**DES KEK key part *{0}* loaded.**

Explanation

Substitution variables are:

*{0}*Key label

5695	**Failure occurred loading DES KEK key part *{0}*.**

Explanation

Substitution variables are:

*{0}*Key label

5696 **DES KEK key part *{0}* replaced existing key part.**

Explanation

Substitution variables are:

*{0}*Key label

5697 **Failure occurred replacing DES KEK key part *{0}*.**

Explanation

Substitution variables are:

*{0}*Key label

5698 **PKA key storage initialized to *{0}* by *{1}*.**

Explanation

Substitution variables are:

*{0}*File name
*{1}*Caller

5699 **DES key storage initialized to *{0}* by *{1}*.**

Explanation

Substitution variables are:

*{0}*File name
*{1}*Caller

5700 **AES key storage initialized to *{0}* by *{1}*.**

Explanation

Substitution variables are:

*{0}*File name
*{1}*Caller

Messages 5701-5800

5701 **Failed to initialize PKA key storage.**

5702 **Failed to initialize DES key storage.**

5703 **Failed to initialize AES key storage.**

5704 **Key records in *{0}* key storage were re-enciphered.**

Explanation

Substitution variables are:

*{0}*Storage type

5705 ***{0}* key storage re-encipher failure.**

Explanation

Substitution variables are:

*{0}*Storage type

5706 **Key record in *{0}* key storage created.**

Explanation

Substitution variables are:

*{0}*Storage type

5707 ***{0}* key storage record create failure.**

Explanation

Substitution variables are:

*{0}*Key type

5708 ***{0}* key storage record deleted.**

Explanation

Substitution variables are:

*{0}*Key type

5709 ***{0}* key storage record delete failure.**

Explanation

Substitution variables are:

*{0}*Key type

5720 **Workstation crypto adapter *{0}* master *{1}* set.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Key(s)

5721 **Workstation crypto adapter *{0}* master *{1}* set failed.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Key(s)

5722 **Workstation crypto adapter random *{0}* master keys set.**

Explanation

Substitution variables are:

*{0}*Key type

5723 **Workstation crypto adapter random *{0}* master keys set failed.**

Explanation

Substitution variables are:

*{0}*Key type

5724 **Workstation crypto adapter new *{0}* master *{1}* successfully cleared.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Key(s)

5725 **Workstation crypto adapter clear new *{0}* master *{1}* failed.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Key(s)

5726 ***{0}* *{1}* master key part opened from *{2}*.**

Explanation

Substitution variables are:

*{0}*Key part
*{1}*Key type
*{2}*File name

5727 **Failure occurred opening *{0}* master key part from *{1}*.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*File name

5728 **Workstation crypto adapter *{0}* master key part loaded.**

Explanation

Substitution variables are:

*{0}*Key type

5729 **Workstation crypto adapter *{0}* master key load failure.**

Explanation

Substitution variables are:

*{0}*Key type

5730 ***{0}* master key part saved to *{1}*.**

Explanation

Substitution variables are:

*{0}*Key type
*{1}*File name

5731 ***{0}* master key save failure.**

Explanation

Substitution variables are:

*{0}*Key type

5732 **Workstation crypto adapter *{0} {1}* master key part loaded from smart card, *{2}* (*{3}*).**

Explanation

Substitution variables are:

*{0}*Key part
*{1}*Register type
*{2}*Card name
*{3}*Card identifier

5733 **Workstation crypto adapter *{0}* master key part failed to load from smart card *{1}* (*{2}*).**

Explanation

Substitution variables are:

*{0}*Register type
*{1}*Card name
*{2}*Card identifier

5734 ***{0} {1}* workstation crypto adapter master key part generated on smart card, *{2}* (*{3}*).**

Explanation

Substitution variables are:

*{0}*Key part
*{1}*Register type
*{2}*Card name
*{3}*Card identifier

5735 **Workstation crypto adapter *{0}* master key part generation to smart card failed. Card ID: *{1}***

Explanation

Substitution variables are:

*{0}*Register type
*{1}*Card identifier

5740 **Workstation crypto adapter access control initialized.**

5741 **Workstation crypto adapter access control initialize failure.**

5742 **Profile (*{0}*) saved to *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Storage medium

5743 **Profile save failure. *{0}***

Explanation

Substitution variables are:

*{0}*Profile name

5744 **Group profile (*{0}*) saved to *{1}***

Explanation

Substitution variables are:

*{0}*User name
*{1}*Storage medium

5745 **Profile (*{0}*) replaced.**

Explanation

Substitution variables are:

*{0}*User name

5746 **Profile (*{0}*) created.**

Explanation

Substitution variables are:

*{0}*Profile name

5747 **Profile create failure.**

5748 **Group profile (*{0}*) replaced.**

Explanation

Substitution variables are:

*{0}*User name

5749 **Group profile (*{0}*) created.**

Explanation

Substitution variables are:

*{0}*User name

5750 **Profile (*{0}*) failure count reset.**

Explanation

Substitution variables are:

*{0}*User name

5751 **Profile failure count reset failure.**

5752 **Profile (*{0}*) passphrase changed.**

Explanation

Substitution variables are:

*{0}*User name

5753 **Profile passphrase change failure.**

5754 **Profile (*{0}*) deleted.**

Explanation

Substitution variables are:

*{0}*User name

5755 **Profile delete failure.**

5756 **Deleting group profile (*{0}*).**

Explanation

Substitution variables are:

*{0}*User name

5757 **Profile (*{0}*) opened from *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*File name

5758 **Group profile (*{0}*) opened from *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*File name

5759 **Failure occurred opening profile from *{0}***

Explanation

Substitution variables are:

*{0}*File name

5770 **Role (*{0}*) deleted.**

Explanation

Substitution variables are:

*{0}*Role identifier

5771 **Role delete failure.**

5772 **Role (*{0}*) saved to *{1}*.**

Explanation

Substitution variables are:

*{0}*Role identifier
*{1}*File name

5773 **Role Save Failure. (*{0}*)**

Explanation

Substitution variables are:

*{0}*Save error

5774 **Role (*{0}*) loaded to TKE workstation crypto adapter.**

Explanation

Substitution variables are:

*{0}*Role identifier

5775 **Load role failure.**

5776 ***{0}* (*{1}*) PIN changed.**

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Card identifier

5777 **Smart card PIN change failure.**

5778 **A *{0}* was copied to a smart card. Source card ID: *{1}*, Source zone ID: *{2}*, Target card ID: *{3}*, Target zone ID: *{4}***

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Card identifier
*{2}*Source zone identifier
*{3}*Target card identifier
*{4}*Target zone identifier

5779 **Failure during smart card copy. Source card ID: *{0}*, Source zone ID: *{1}*, Target card ID: *{2}*, Target zone ID: *{3}***

Explanation

Substitution variables are:

*{0}*Source card identifier
*{1}*Source zone identifier
*{2}*Target card identifier
*{3}*Target zone identifier

5780 **A logon key pair was generated on *{0}* (*{1}*).**

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Card identifier

5781 **A logon key pair generation failure occurred.**

5782 **A *{0}* was deleted from a smart card. Card ID: *{1}*, Zone ID: *{2}***

Explanation

Substitution variables are:

*{0}*Key type
*{1}*Card identifier
*{2}*Zone identifier

5783 **Failure during smart card delete. Card ID: *{0}*, Zone ID: *{1}***

Explanation

Substitution variables are:

*{0}*Card identifier
*{1}*Zone identifier

5800 **Smart card utility program - Started**

Messages 5801-5900

5801 **Smart card utility program - Start failed**

5802 **Smart card utility program - Exited**

5803 **Smart card utility program - Exit failed**

5804 **Failure getting smart card description.\nError Code: *{0}***

Explanation

Substitution variables are:

*{0}*Error code

5805 **Failure getting PIN information.\nError Code: *{0}***

Explanation

Substitution variables are:

*{0}*Error code

5806 **Failure getting zone information.\nError Code: *{0}***

Explanation

Substitution variables are:

*{0}*Error code

5807 **Failure getting authority information.\nError Code: *{0}***

Explanation

Substitution variables are:

*{0}*Error code

5808 **Failure querying for key parts.**

5809 **Failure getting crypto adapter logon information.\nError Code: *{0}***

Explanation

Substitution variables are:

*{0}*Error code

5810 ***{0}* PIN was set or changed on *{1}*. Card ID: *{2}*, Card description: *{3}*.**

Explanation

Substitution variables are:

*{0}*Pin position
*{1}*Card type
*{2}*Card identifier
*{3}*Card description

5811 **Failed to set or change the PIN on *{0}*.**

Explanation

Substitution variables are:

*{0}*Smart card type

5812 **The PIN was unblocked on *{0}*. Card ID: *{1}*, Card Description: *{2}*.**

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Card identifier
*{2}*Card description

5813 **Failure occurred unblocking *{0}* PIN.**

Explanation

Substitution variables are:

*{0}*Smart card type

5814 **Successfully backed up *{0}*. Source card ID: *{1}*, Source card description: *{2}*, Target card ID: *{3}*, Zone ID: *{4}*, Zone description: *{5}*.**

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Source identifier
*{2}*Source description
*{3}*Target identifier

*{4}*Zone identifier
*{5}*Zone description

5815 **Failed to back up *{0}*.**

Explanation

Substitution variables are:

*{0}*Smart card type

5816 ***{0}* initialization complete. Card ID: *{1}*, Zone ID: *{2}*, Zone description: *{3}*.**

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Card identifier
*{2}*Zone identifier
*{3}*Zone description

5817 **Failure occurred initializing *{0}*.**

Explanation

Substitution variables are:

*{0}*Smart card type

5818 ***{0}* has been personalized. Card ID: *{1}*, Card description: *{2}*.**

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Card identifier
*{2}*Card description

5819 **Failed to personalize *{0}*.**

Explanation

Substitution variables are:

*{0}*Card type

5820 ***{0}* initialization complete. Card description: *{1}*, Card ID: *{2}*, Zone ID: *{3}*, Zone description: *{4}*.**

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Card description
*{2}*Card identifier
*{3}*Zone identifier
*{4}*Zone description

5821 **Failure occurred initializing *{0}*.**

Explanation

Substitution variables are:

*{0}*Smart card type

5822	***{0}* enrollment with crypto adapter.**

Explanation

Substitution variables are:

*{0}*Location

5823	**Started ...**
5824	**Completed successfully.**
5825	**TKE smart card (*{0}*) enrolled in zone (*{1}*) successfully.**

Explanation

Substitution variables are:

*{0}*Card name
*{1}*Zone identifier

5826	**TKE smart card enrollment with crypto adapter failed.**
5827	**Enrollment request from *{0}* for crypto adapter *{1}* was certified by CA smart card (*{2}*) and enrolled in zone (*{3}*)**

Explanation

Substitution variables are:

*{0}*File name
*{1}*Serial number
*{2}*Card identifier
*{3}*Zone identifier

5828	**Saved enrollment request file to *{0}*.**

Explanation

Substitution variables are:

*{0}*File name

5829	**Remote enroll with crypto adapter.**
5830	**Remote enroll with crypto adapter failed.**
5831	**Begin remote enroll - Started**
5832	**Begin remote enroll - Failed\nError Code: *{0}***

Explanation

Substitution variables are:

*{0}*Error code

5833	**User cancelled begin remote enroll**
5834	**Begin remote enroll\nUser is replacing certificate in zone (*{0}*)**

Explanation

Substitution variables are:

*{0}*Zone identifier

5835 **Begin remote enroll\nCrypto adapter enrollment request has been stored in file *{0}***

Explanation

Substitution variables are:

*{0}*File name

5836 **Complete remote enroll - Started**

5837 **Complete remote enroll - Failed\nError Code: *{0}***

Explanation

Substitution variables are:

*{0}*Error code

5838 **User cancelled complete remote enroll**

5839 **Complete remote enroll\nUser is replacing certificate in zone (*{0}*)**

Explanation

Substitution variables are:

*{0}*Zode id

5840 **Complete remote enroll\nCrypto adapter *{0}* enrolled in zone (*{1}*) successfully from file (*{2}*)**

Explanation

Substitution variables are:

*{0}*Crypto adapter name
*{1}*Zone identifier
*{2}*File name

5841 **Enrolled *{0}* in alternate zone. Card ID: *{1}*, Card description: *{2}*, Alternate zone ID: *{3}*, Alternate zone description: *{4}*.**

Explanation

Substitution variables are:

*{0}*Card type name
*{1}*Card identifier
*{2}*Card description
*{3}*Alternate zone identifier
*{4}*Alternate zone description

5842 **Failure enrolling *{0}* in alternate zone.**

Explanation

Substitution variables are:

*{0}*Card type name

5843 **Removed alternate zone from *{0}*. Card ID: *{1}*, Card description: *{2}*.**

Explanation

Substitution variables are:

*{0}*Card type name
*{1}*Card identifier
*{2}*Card description

5844 **Failure removing alternate zone from *{0}*.**

Explanation

Substitution variables are:

*{0}*Card type name

5845 **Local crypto adapter unenrollment.**

5846 **Unenrollment completed successfully.**

5847 **Unenrollment failed.**

5900 **The TKE audit configuration utility opened.**

Messages 5901-6000

5901 **The TKE audit configuration utility failed to open.**

5902 **The TKE audit configuration utility closed.**

5903 **The TKE audit configuration utility failed to close.**

5904 **The TKE audit configuration utility was modified.**

5905 **The auditing function for TKE was started.**

5906 **The auditing function for TKE was stopped.**

5907 **File *{0}* by the edit TKE files task.**

Explanation

Substitution variables are:

*{0}*File function

5908 **An error was encountered while opening the edit TKE files task: *{0}***

Explanation

Substitution variables are:

*{0}*Error message

5909 **Migrate previous TKE Version to TKE 8.1 task completed successfully.**

5910 **Migrate previous TKE Version to TKE 8.1 task failed: *{0}***

Explanation

Substitution variables are:

*{0}*Error message

5911 **The TKE file management utility opened.**

5912 **The TKE file management utility closed.**

5913 **The TKE file management utility failed to open.**

5914 **The TKE file management utility failed to close.**

5915 **File *{0}*.**

Explanation

Substitution variables are:

*{0}*File name

5916 **File copy failed: *{0}***

Explanation

Substitution variables are:

*{0}*Error message

5917 **The TKE restricted file chooser was opened.**

5918 **The TKE restricted file chooser failed to open.**

5919 **File *{0}* was saved to *{1}*.**

Explanation

Substitution variables are:

*{0}*File name
*{1}*Directory name

5920 **File save failed: *{0}***

Explanation

Substitution variables are:

*{0}*File name

5921 **File *{0}* from *{1}* was opened.LPAR_SEC_EXECUTION_ON**

Explanation

Substitution variables are:

*{0}*File name
*{1}*Directory name

5922 **File open failed: *{0}***

Explanation

Substitution variables are:

*{0}*Rile name

5923 **File *{0}* was deleted from *{1}*.**

Explanation

Substitution variables are:

*{0}*File name
*{1}*Directory name

5924 **File delete failed: *{0}***

Explanation

Substitution variables are:

*{0}*File name

5925 **File *{0}* was renamed to *{2}* in the *{1}*.**

Explanation

Substitution variables are:

*{0}*Old file name
*{1}*Directory name
*{2}*New file name

5926 **File rename failed: *{0}***

Explanation

Substitution variables are:

*{0}*File name

5927 **The TKE audit record upload configuration utility was opened.**

5928 **The TKE audit record upload configuration utility failed to open.**

5929 **The TKE audit record upload configuration utility was closed.**

5930 **The TKE Audit record upload configuration utility failed to close.**

5931 **TKE Audit record upload settings were modified. *{0}***

Explanation

Substitution variables are:

*{0}*Upload setting

5932 **Failure modifying TKE audit record upload settings.**

5933 **The saved upload timestamp for host *{0}* was reset.**

Explanation

Substitution variables are:

*{0}*Host name

5934 **Host *{0}* was removed from the list of other hosts.**

Explanation

Substitution variables are:

*{0}*Host name

5935 ***{0}*** **was made the current host for audit uploads.**

Explanation

Substitution variables are:

*{0}*Host name

5936 **Host *{0}* was removed as the current host. No current host is selected.**

Explanation

Substitution variables are:

*{0}*Host name

5937 **The upload timestamp for the current host (*{0}*) was reset.**

Explanation

Substitution variables are:

*{0}*Host name

5938 **Host *{0}* was added to the list of other hosts.**

Explanation

Substitution variables are:

*{0}*Host name

5939 **Autostart of audit record upload was enabled.**

5940 **Autostart of audit record upload was disabled.**

5941 **Audit record upload to system *{0}* has started.**

Explanation

Substitution variables are:

*{0}*Host port

5942 **Audit record upload to system *{0}* failed. Status: *{1}*.**

Explanation

Substitution variables are:

*{0}*Host port
*{1}*Status

5943 **Audit record upload to system *{0}* has stopped.**

Explanation

Substitution variables are:

*{0}*Host port

5944 **Audit record upload to system *{0}* failed to stop.**

Explanation

Substitution variables are:

*{0}*Host port

5945	**The TKE configure displayed hash size utility was opened.**
5946	**The TKE configure displayed hash size utility failed to open.**
5947	**The TKE configure displayed hash size utility was closed.**
5948	**The TKE configure displayed hash size utility failed to close.**
5949	**The displayed hash size configuration was changed. *{0}***

Explanation

Substitution variables are:

*{0}*Displayed hash setting

5950	**Attempt to modify displayed hash size configuration failed: *{0}***

Explanation

Substitution variables are:

*{0}*Displayed hash setting

5951	**Hash truncation was enabled, and the maximum displayed hash size was set to *{0}*.**

Explanation

Substitution variables are:

*{0}*Hash size

5952	**Hash truncation was disabled, and full hashes will be displayed.**
5953	**The z/OS enhanced password encryption policy was enabled.**
5954	**The z/OS enhanced password encryption policy was disabled.**
5955	**The z/OS enhanced password encryption policy utility was opened.**
5956	**The z/OS enhanced password encyrption policy utility was closed.**
5960	**An error was encountered while reading audit records due to incorrect parameters specified.**
5961	**An error was encountered while writing an audit record due to incorrect parameters specified.**
5962	**Heartbeat audit records will be created.**
5963	**Heartbeat audit interval *{0}* is not one of the pre-defined intervals.**

Explanation

Substitution variables are:

*{0}*Heartbeat interval in error

5964	**The TKE crypto adapter intrusion latch state has changed.**
5965	**The TKE workstation has started.**
5966	**A different TKE crypto adapter has been detected.**

5967	**Heartbeat audit record.**
5968	**Cannot connect to the TKE crypto adapter to check the crypto adapter serial number. There may not be a crypto adapter installed, the crypto adapter may not be reporting in, or the CLU utility may be running.**
5969	**The TKE crypto adapter battery level has changed.**
5970	**The TKE OA signature policy was updated. Original policy: require ECC OA signatures = *{0}*, require Dilithium OA signatures = *{1}*. New policy: require ECC OA signatures = *{2}*, require Dilithium OA signatures = *{3}*.**

Explanation

Substitution variables are:

*{0}*Original value of ECC OA signature policy
*{1}*Original value of Dilithium OA signature policy
*{2}*New value of ECC OA signature policy
*{3}*New value of Dilithium OA signature policy

5997	**TKE audit record\n- TKE workstation profile: *{1}*\n- TKE crypto adapter profile: *{2}*\n- Authority index *{3}*, Key ID:\n*{4}*\n- Event information: *{0}***

Explanation

Substitution variables are:

*{0}*Event information
*{1}*TKE workstation profile
*{2}*Crypto adapter profile
*{3}*Authority index
*{4}*Key identifier

5998	**TKE audit record\n- TKE workstation profile: *{1}*\n- TKE crypto adapter profile: *{2}*\n- Authority index *{3}*, Key ID: *{4}*\n- Event information: *{0}***

Explanation

Substitution variables are:

*{0}*Event information
*{1}*TKE workstation profile
*{2}*Crypto adapter profile
*{3}*Authority index
*{4}*Key identifier

5999	**TKE Audit Record\n- TKE Workstation Profile: *{1}*\n- TKE Crypto Adapter Profile: *{2}*\n- Event Information: *{0}***

Explanation

Substitution variables are:

*{0}*Event information
*{1}*TKE Workstation profile
*{2}*Crypto adapter profile

Messages 6001-6100

6001 **RSF initiated an SSL connection with host *{1}* at address *{3}* authenticated as *{0}* with encryption cipher *{2}***

Explanation

Substitution variables are:

*{0}*Principal name
*{1}*Host name
*{2}*Cipher suite name
*{3}*IP address

6002 **RSF connection failed verification of server certificate at *{0}*, reason: *{1}***

Explanation

Substitution variables are:

*{0}*Host name
*{1}*Failure reason

6003 **RSF initiated an SSL connection with host *{0}***

Explanation

Substitution variables are:

*{0}*Host name

6005 **Call home connection for request *{0}* canceled.**

Explanation

Substitution variables are:

*{0}*Request description

6006 **Call home connection for request *{0}* released.**

Explanation

Substitution variables are:

*{0}*Request description

6007 **RSF request *{0}* will transmit *{1}* files to the Support System. The files may be compressed archives which contain other files that are not currently listed in this entry. The files are as follows:**

Explanation

Substitution variables are:

*{1}*Request description
*{2}*Number of files

6008 **Call home review has been configured to hold the following types of requests: \n *{0}***

Explanation

Substitution variables are:

*{0}*List of held request types

6009 **RSF request *{0}* will transmit no files to the support system.**

Explanation

Substitution variables are:

*{0}*Request description

6051 **A web services client on *{0}* attempted an unauthorized (*{1}*) action "*{2}*" as *{3}* against the *{4}* object named "*{5}*" (URI:*{6}*)**

Explanation

Substitution variables are:

*{0}*The IP address, if available, of the client
*{1}*The HTTP response returned to the client
*{2}*A description of the attempted action
*{3}*The user that was logged in
*{4}*The type of object that was targeted
*{5}*The displayable name of the targeted object (i.e 'Blade 1' or 'Blade 1 within enclosure Foo')
*{6}*The URI being rejected

6052 **A web services client on *{0}* attempted an unauthorized (*{1}*) action "*{2}*" as *{3}* against the *{4}* object named "*{5}*": *{6}* (URI:*{7}*)**

Explanation

Substitution variables are:

*{0}*The IP address, if available, of the client
*{1}*The HTTP response returned to the client
*{2}*A description of the attempted action
*{3}*The user that was logged in
*{4}*The type of object that was targeted
*{5}*The displayable name of the targeted object (i.e 'Blade 1' or 'Blade 1 within enclosure Foo')
*{6}*Provider specific details
*{7}*The URI being rejected

6053 **A web services client on *{0}* attempted an unauthorized (*{1}*) action "*{2}*" as *{3}* against the *{4}* object named "*{5}*". User does not have permission to the *{6}* named "*{7}*" (URI:*{8}*)**

Explanation

Substitution variables are:

*{0}*The IP address, if available, of the client
*{1}*The HTTP response returned to the client
*{2}*A description of the attempted action
*{3}*The user that was logged in
*{4}*The type of object that was targeted
*{5}*The displayable name of the targeted object (i.e 'Blade 1' or 'Blade 1 within enclosure Foo')
*{6}*The type of entity associated with the rejection (typically a 'Task')
*{7}*The displayable name of the entity associated with the rejection
*{8}*The URI being rejected

6054 **A web services client on *{0}* attempted an unauthorized (*{1}*) action "*{2}*" as *{3}*. User does not have permission to the *{4}* named "*{5}*" (URI:*{6}*)**

Explanation

Substitution variables are:

*{0}*The IP address, if available, of the client
*{1}*The HTTP response returned to the client
*{2}*A description of the attempted action
*{3}*The user that was logged in
*{4}*The type of entity associated with the rejection (typically a 'Task')
*{5}*The displayable name of the entity associated with the rejection
*{6}*The URI being rejected

6055 **A web services client on *{0}* attempted an unauthorized (*{1}*) action "*{2}*" as *{3}*: *{4}* (URI:*{5}*)**

Explanation

Substitution variables are:

*{0}*The IP address, if available, of the client
*{1}*The HTTP response returned to the client
*{2}*A description of the attempted action
*{3}*The user that was logged in
*{4}*Provider specific details
*{5}*The URI being rejected

6060 **A request was made by user *{0}* to change the Licensed Internal Code security mode from *{1}* to *{2}*.**

Explanation

Substitution variables are:

*{0}*Username of request initiator
*{1}*Previous Licensed Internal Code security mode
*{2}*New Licensed Internal Code security mode

6061 **An attempt to change the Licensed Internal Code Security mode on the *{0}* from *{1}* to *{2}* has failed.**

Explanation

Substitution variables are:

*{0}*Primary or Alternate system
*{1}*Previous Licensed Internal Code security mode
*{2}*New Licensed Internal Code security mode

6062 **The Licensed Internal Code security mode is *{0}*.**

Explanation

Substitution variables are:

*{0}*Current Licensed Internal Code security mode

6063 **The Primary Licensed Internal Code security mode is *{0}*. The Alternate Licensed Internal Code security mode is *{1}*.**

Explanation

Substitution variables are:

*{0}*Primary Licensed Internal Code security mode
*{1}*Alternate Licensed Internal Code security mode

6070 **Success importing Product Engineering access control file.**

6071 **Failure importing Product Engineering access control file with error: *{0}***

Explanation

Substitution variables are:

*{0}*Detailed error for access control file import failure

6072 **Success removing Product Engineering access control file.**

6073 **Success removing Product Engineering access control file due to expiration.**

6100 **PDU service state has been enabled.**

Messages 6101-6200

6101 **PDU service state has been disabled.**

6111 **A Change LPAR Group controls scheduled operation was started from *{0}.{1}*.**

Explanation

Substitution variables are:

*{0}*NAU
*{1}*Network ID

6112 **Logical partition group control settings were changed by a scheduled operation.**

6120 **Speed boost is on for partition *{0}*, partition number *{1}*. Active boost type is *{2}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Partition number
*{2}*ActiveBoostType

6121 **Speed boost is off for partition *{0}*, partition number *{1}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Partition number

6122 **zIIP capacity boost is on for partition *{0}*, partition number *{1}*. Active boost type is *{2}*.**

Explanation

Substitution variables are:

*{0}*doc=Image name
*{1}*Partition number
*{2}*ActivePoolType

6122 **zAAP capacity boost is off for partition *{0}*, partition number *{1}*.**

Explanation

Substitution variables are:

*{0}*doc=Image name
*{1}*Partition number

6123 **zIIP capacity boost is off for partition *{0}*, partition number *{1}*.**

Explanation

Substitution variables are:

*{0}*doc=Image name
*{1}*Partition number

6124 **Secure Execution for Linux is on for partition *{0}*, partition number *{1}*.**

Explanation

Substitution variables are:

*{0}*doc=Image name
*{1}*Partition number

6125 **Secure Execution for Linux is off for partition *{0}*, partition number *{1}*.**

Explanation

Substitution variables are:

*{0}*Image name
*{1}*Partition number

6126 **Multiple HMC users with different properties match the user name *{0}* and associated password. Unable to provide a user due to this collision on HMCs *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*HMC names

6127 **Multiple HMC users with equal properties match the user name *{0}* and associated password. Providing the user from HMC *{1}* which has recently communicated. Matching credentials found on HMCs *{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*HMC name user was provided from
*{2}*All HMC names considered

6128 **A single user was found matching the user name *{0}* and associated password from HMC *{1}*. Providing the user.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*HMC name

6129 **An error occurred during logon for user *{0}* while attempting to authenticate an additional factor.**

Explanation

Substitution variables are:

*{0}*User name

6130 **An error occurred during logon for user *{0}* while attempting to authenticate using IBM MFA through *{1}* MFA server *{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Indication of 'primary' or 'backup' MFA server
*{2}*MFA server name

6131 **An error occurred during logon for user *{0}* while attempting to provide more information in response to an IBM MFA server NMI request through *{1}* MFA server *{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Indication of 'primary' or 'backup' MFA server
*{2}*MFA server name

6132 **Secure Execution for Linux is enabled for system *{0}*. The global key is *{1}*, the host key is *{2}* and the host import key is *{3}*.**

Explanation

Substitution variables are:

*{0}*Cpc name
*{1}*global key installed
*{2}*host key installed
*{3}*host import key installed

6133 **Secure Execution for Linux is disabled for system *{0}*.**

Explanation

Substitution variables are:

*{0}*Cpc name

6134 ***{0}* secondary key for Secure Execution was deleted. The secondary hash removed from i390 is *{1}*.**

Explanation

Substitution variables are:

*{0}*Secure execution key type.
*{1}*Computed hash of the secure execution secondary key.

6135 ***{0}* primary key for Secure Execution was successfully installed. The primary hash retrieved from i390 is *{1}*.**

Explanation

Substitution variables are:

*{0}*Secure execution key type.
*{1}*Computed hash of the secure execution primary key.

6136 ***{0}* key roll for Secure Execution starts a new grace period.**

Explanation

Substitution variables are:

*{0}*Secure execution key type.

6137 ***{0}* key roll for Secure Execution aborts current grace period.**

Explanation

Substitution variables are:

*{0}*Secure execution key type

6138 **Secure Execution key hashes currently on system. The primary host key hash is *{0}*, the secondary host key hash is *{1}*, the primary global key hash is *{2}*, the secondary global key hash is *{3}*.**

Explanation

Substitution variables are:

*{0}*Computed hash of the primary host key bundle.
*{1}*Computed hash of the secondary host key bundle.
*{2}*Computed hash of the primary global hyper protect key bundle.
*{3}*Computed hash of the secondary global hyper protect key bundle.

6140 **User *{0}* successfully started the Recovery Console Boot Server on interface(s) *{1}* using ISO file *{2}* for client with name *{3}*, system type *{4}*, and MAC address(es) *{5}*.**

Explanation

Substitution variables are:

*{0}*user name of user that started server
*{1}*server interface(s) involved in recovery
*{2}*ISO file name being used in recovery
*{3}*name of client system
*{4}*type of client system
*{5}*client MAC address(es) involved in recovery

6141 **User *{0}* successfully started the Recovery Console Boot Server on interface(s) *{1}* using ISO file *{2}* for client with MAC address(es) *{3}*.**

Explanation

Substitution variables are:

*{0}*user name of user that started server
*{1}*server interface(s) involved in recovery
*{2}*ISO file name being used in recovery
*{3}*client MAC address(es) involved in recovery

6142 **User *{0}* successfully stopped the Recovery Console Boot Server that was running on interface(s) *{1}* using ISO file *{2}* for client with name *{3}*, system type *{4}*, and MAC address(es) *{5}*.**

Explanation

Substitution variables are:

*{0}*user name of user that stopped server
*{1}*server interface(s) involved in recovery
*{2}*ISO file name being used in recovery
*{3}*name of client system
*{4}*type of client system
*{5}*client MAC address(es) involved in recovery

6143 **User *{0}* successfully stopped the Recovery Console Boot Server that was running on interface(s) *{1}* using ISO file *{2}* for client with MAC address(es) *{3}*.**

Explanation

Substitution variables are:

*{0}*user name of user that stopped server
*{1}*server interface(s) involved in recovery
*{2}*ISO file name being used in recovery
*{3}*client MAC address(es) involved in recovery

6144 **User *{0}* failed to start the Recovery Console Boot Server on interface(s) *{1}* using ISO file *{2}* for client with name *{3}*, system type *{4}*, and MAC address(es) *{5}*. Failure message: *{6}***

Explanation

Substitution variables are:

*{0}*user name of user that attempted to start server
*{1}*server interface(s) involved in recovery
*{2}*ISO file name being used in recovery
*{3}*name of client system
*{4}*type of client system
*{5}*client MAC address(es) involved in recovery
*{6}*error messsage received from server code

6145 **User *{0}* failed to start the Recovery Console Boot Server on interface(s) *{1}* using ISO file *{2}* for client with MAC address(es) *{3}*. Failure message: *{4}***

Explanation

Substitution variables are:

*{0}*user name of user that attempted to start server
*{1}*server interface(s) involved in recovery
*{2}*ISO file name being used in recovery
*{3}*client MAC address(es) involved in recovery

*{4}*error message received from server code

6150 **The passwords for the default users *{0}* were reset to their default values by *{1}*. These default users will be required to change their passwords the next time they log in.**

Explanation

Substitution variables are:

*{0}*User names
*{1}*Name of the current user

6151 **The password for the SERVICE user has been reset to its default value by *{1}*. The default users *{0}* will be required to change their passwords the next time they log in.**

Explanation

Substitution variables are:

*{0}*User names
*{1}*Name of the current user

6152 **The user *{0}* has begun the process of changing their password.**

Explanation

Substitution variables are:

*{0}*User name

6153 **An IBM Z MFA server definition named *{0}* has been created.**

Explanation

Substitution variables are:

*{0}*MFA server definition name

6154 **An IBM Z MFA server definition named *{0}* has been modified.**

Explanation

Substitution variables are:

*{0}*MFA server definition name

6155 **An IBM Z MFA server definition named *{0}* has been deleted.**

Explanation

Substitution variables are:

*{0}*MFA server definition name

6160 **Proxied connection initiated to *{0}* on behalf of *{1}*.**

Explanation

Substitution variables are:

*{0}*the proxied connection destination
*{1}*the proxied connection originator

6161 **Proxied connection handler initiated to *{0}* on behalf of *{1}* using SSL.**

Explanation

Substitution variables are:

*{0}*the proxied connection destination
*{1}*the proxied connection originator

6165 **Console certificate expiring in *{2}* day(s) or less. It will expire on *{0}*. The common name is *{1}*.**

Explanation

Substitution variables are:

*{0}*Expiration date
*{1}*Common name
*{2}*Expiring in x days

6166 **Console certificate has expired. It has expired on *{0}*.**

Explanation

Substitution variables are:

*{0}*Expiration date

6167 **Generic certificate expiring in *{2}* day(s) or less. It will expire on *{0}*. The common name is *{1}*.**

Explanation

Substitution variables are:

*{0}*Expiration date
*{1}*Common name
*{2}*Expiring in x days

6168 **Generic certificate has expired. It has expired on *{0}*.**

Explanation

Substitution variables are:

*{0}*Expiration date

6169 **EDiF certificate expiring in *{1}* day(s) or less. It will expire on *{0}*.**

Explanation

Substitution variables are:

*{0}*Expiration date
*{1}*Expiring in x days

6170 **EDiF certificate has expired. It has expired on *{0}*.**

Explanation

Substitution variables are:

*{0}*Expiration date

6171 **Console certificate was expiring within 30 days. It has been auto-replaced.**

6172 **The user *{0}* is required to change their password during logon, but User Profile data cannot be modified on a data replication console with a role of replica. User must login on an HMC which has a data replication role of primary or peer.**

Explanation

Substitution variables are:

*{0}*User name

6173 **The user *{0}* is required to setup HMC MFA during logon, but User Profile data cannot be modified on a data replication console with a role of replica. User must login on an HMC which has a data replication role of primary or peer.**

Explanation

Substitution variables are:

*{0}*User name

6174 **User *{0}* logon failed. Located LDAP entry contains multiple values for the template name override attribute *{2}* fetched from LDAP server *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*LDAP server name
*{2}*Template name override attribute

6175 **User *{0}* logon failed. Template name override attribute *{2}* fetched from LDAP server *{1}* does not contain a User Template name, and no default User Template is specified in the User Pattern *{3}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*LDAP server name
*{2}*Template name override attribute
*{3}*User Pattern name

6176 **User *{0}* logon failed. The user is not a member of any group specified in User Pattern *{1}*, and no default User Template is specified.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*User Pattern name

6177 **User *{0}* logon failed. The LDAP server *{1}* specified in the User Template is unknown.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*LDAP server name

6178 **User *{0}* logon failed. The User Template *{1}* bound to User Pattern *{2}* does not exist.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*User Template name
*{2}*User Pattern name

6179 **User *{0}* logon failed. The LDAP Server Definition *{1}* has an invalid distinguished name pattern *{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*LDAP Server Definition
*{2}*DN Pattern

6180 **User *{0}* logon failed. The User Template *{2}* specified in LDAP attribute *{3}* fetched from the LDAP server *{1}* does not exist.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*LDAP server name
*{2}*User Template name
*{3}*LDAP attribute name

6181 **User *{0}* logon failed. The User Template *{1}* specified in User Pattern *{2}* does not exist.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*Template name
*{2}*User Pattern Name

6182 **User *{0}* logon failed. Unable to authenticate to LDAP server *{1}* using the initial bind information to verify the user.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*LDAP server name

6184 **User *{0}* logon failed. Unable to locate a unique LDAP directory entry using LDAP server *{1}*. The search returned multiple results. *{2}***

Explanation

Substitution variables are:

*{0}*User name

*{1}*LDAP server name
*{2}*Exception details

6185 **User *{0}* logon failed. The LDAP server *{1}* took too long to respond to the search request. *{2}***

Explanation

Substitution variables are:

*{0}*User name
*{1}*LDAP server name
*{2}*Exception details

6186 **User *{0}* logon failed. Unexpected error contacting LDAP server *{1}* for authentication. *{2}***

Explanation

Substitution variables are:

*{0}*User name
*{1}*LDAP server name
*{2}*Exception details

6187 **User *{0}* logon failed. Unable to locate the LDAP directory entry for user *{1}* using LDAP server *{2}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*User name
*{2}*LDAP server name

6188 **User *{0}* logon failed. Distinguished name *{2}* does not exist in the LDAP directory managed by LDAP server *{1}*.**

Explanation

Substitution variables are:

*{0}*User name
*{1}*LDAP server name
*{2}*Distinguished name

6189 **User *{0}* logon failed. The user is not permitted to log on to management consoles in this domain.**

Explanation

Substitution variables are:

*{0}*User name

6190 **User *{0}* logon failed. Error contacting LDAP server for authentication. *{1}***

Explanation

Substitution variables are:

*{0}*User name
*{1}*Exception details

6191 **User *{0}* logon failed. Unable to negotiate a secure connection to the LDAP server *{1}*. *{2}***

Explanation

Substitution variables are:

*{0}*User name
*{1}*LDAP server name
*{2}*Exception details

6192 **User *{0}* logon failed. Unable to negotiate a secure connection to the LDAP server *{1}*. The LDAP server's certificate is not trusted. *{2}***

Explanation

Substitution variables are:

*{0}*User name
*{1}*LDAP server name
*{2}*Exception details

6193 **User *{0}* logon failed. Unable to locate a required LDAP directory entry during search using LDAP server *{1}*. Remaining name: *{2}***

Explanation

Substitution variables are:

*{0}*User name
*{1}*LDAP server name
*{2}*Remaining name

6194 **User *{0}* logon failed. The user's credentials verified by LDAP server *{1}* are incorrect. *{2}***

Explanation

Substitution variables are:

*{0}*User name
*{1}*LDAP server name
*{2}*Exception details

6195 **User *{0}* logon failed. An error occurred on both the primary and secondary LDAP servers. The error on the primary LDAP server was: the LDAP server *{1}* took too long to respond to the search request. *{2}***

Explanation

Substitution variables are:

*{0}*User name
*{1}*LDAP server name
*{2}*Exception details

6196 **User *{0}* logon failed. An error occurred on both the primary and secondary LDAP servers. The error on the primary LDAP server was: error contacting LDAP server for authentication. *{1}***

Explanation

Substitution variables are:

*{0}*User name
*{1}*Exception details

6197 **User *{0}* logon failed. An error occurred on both the primary and secondary LDAP servers. The error on the primary LDAP server was: unable to negotiate a secure connection to the LDAP server *{1}*. *{2}***

Explanation

Substitution variables are:

*{0}*User name
*{1}*LDAP server name
*{2}*Exception details

6198 **User *{0}* logon failed. An error occurred on both the primary and secondary LDAP servers. The error on the primary LDAP server was: unable to negotiate a secure connection to the LDAP server *{1}*. The LDAP server's certificate is not trusted. *{2}***

Explanation

Substitution variables are:

*{0}*User name
*{1}*LDAP server name
*{2}*Exception details

6199 **User *{0}* logon failed. An error occurred on both the primary and secondary LDAP servers. The error on the primary LDAP server was: unexpected error contacting LDAP server *{1}* for authentication. *{2}***

Explanation

Substitution variables are:

*{0}*User name
*{1}*LDAP server name
*{2}*Exception details

6200 **User *{0}* logon failed. An error occurred on both the primary and secondary LDAP servers. The error on the primary LDAP server was: unable to locate a unique LDAP directory entry using LDAP server *{1}*. The search returned multiple results. *{2}***

Explanation

Substitution variables are:

*{0}*User name
*{1}*LDAP server name
*{2}*Exception details

Messages 7001-7100

7000 **Profile *{0}* of type *{1}* was created on the system.**

Explanation

Substitution variables are:

*{0}*Profile Name
*{1}*Profile Type

7001 **Profile *{0}* of type *{1}* was deleted from the system.**

Explanation

Substitution variables are:

*{0}*Profile Name
*{1}*Profile Type

7002 **Profile *{0}* of type *{1}* was modified on the system.**

Explanation

Substitution variables are:

*{0}*Profile Name
*{1}*Profile Type

Additional Product Information

Accessibility, feedback information, notices and trademarks about this product can be found here.

Accessibility

Accessible publications for this product are offered in EPUB format and can be downloaded from Resource Link at http://www.ibm.com/servers/resourcelink.

If you experience any difficulty with the accessibility of any IBM Z and IBM LinuxONE information, go to Resource Link at http://www.ibm.com/servers/resourcelink and click **Feedback** from the navigation bar on the left. In the **Comments** input area, state your question or comment, the publication title and number, choose **General comment** as the category and click **Submit**. You can also send an email to reslink@us.ibm.com providing the same information.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Accessibility features

The following list includes the major accessibility features in IBM Z and IBM LinuxONE documentation, and on the Hardware Management Console and Support Element console:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Customizable display attributes such as color, contrast, and font size
- Communication of information independent of color
- Interfaces commonly used by screen magnifiers
- Interfaces that are free of flashing lights that could induce seizures due to photo-sensitivity.

Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

Consult assistive technologies

Assistive technology products such as screen readers function with our publications, the Hardware Management Console, and the Support Element console. Consult the product information for the specific assistive technology product that is used to access the EPUB format publication or console.

IBM and accessibility

See IBM Human Ability and Accessibility center at http://ibm.com/able for more information about the commitment that IBM has to accessibility.

Accessibility features

The following list includes the major accessibility features in IBM Z documentation:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Customizable display attributes such as color, contrast, and font size
- Communication of information independent of color
- Interfaces commonly used by screen magnifiers
- Interfaces that are free of flashing lights that could induce seizures due to photo-sensitivity.

Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

IBM and accessibility

See the IBM Human Ability and Accessibility Center at http://www.ibm.com/able for more information about the commitment that IBM has to accessibility.

How to send your comments

Your feedback is important in helping to provide the most accurate and high-quality information. Send your comments by using Resource Link at http://www.ibm.com/servers/resourcelink. Click **Feedback** on the navigation bar on the left. You can also send an email to reslink@us.ibm.com. Be sure to include the name of the book, the form number of the book, the version of the book, if applicable, and the specific location of the text you are commenting on (for example, a page number, table number, or a heading).

Notices

This information was developed for products and services that are offered in the USA. This material may be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
USA

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION " AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on http://www.ibm.com/trademark.

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other product and service names might be trademarks of IBM or other companies.

Class A Notices

The following Class A statements apply to this IBM product. The statement for other IBM products intended for use with this product will appear in their accompanying manuals.

Federal Communications Commission (FCC) Statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

United Kingdom Notice

This product may cause interference if used in residential areas. Such use must be avoided unless the user takes special measures to reduce electromagnetic emissions to prevent interference to the reception of radio and television broadcasts.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 2014/30/EU on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55032. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

European Community contact:
IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 (0) 800 225 5423 or +49 (0) 180 331 3233
email: halloibm@de.ibm.com

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Japan Voluntary Control Council for Interference (VCCI) Notice

この装置は、クラス A 機器です。 この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。 この場合には使用者が適切な対策を講ずるよう要求される ことがあります。 ＶＣＣＩ－Ａ

The following is a summary of the Japanese VCCI statement above:

This is a Class A product based on the standard of the VCCI Council. If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

Japan Electronics and Information Technology Industries Association (JEITA) Notice

（一社）電子情報技術産業協会　高調波電流抑制対策実施
要領に基づく定格入力電力値：IBM Documentationの各製品の仕様ページ参照

This statement applies to products less than or equal to 20 A per phase.

高調波電流規格　JIS C 61000-3-2 適合品

These statements apply to products greater than 20 A, single-phase.

高調波電流規格　JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
回路分類：6（単相、ＰＦＣ回路付）
換算係数：0

These statements apply to products greater than 20 A per phase, three-phase.

高調波電流規格　JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
回路分類　：5（3相、ＰＦＣ回路付）
換算係数　：0

People's Republic of China Notice

警告:在居住环境中,运行此设备可能会造成无线电干扰。

Declaration: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may need to perform practical action.

Taiwan Notice

CNS 13438:

警告使用者：
此為甲類資訊技術設備，
於居住環境中使用時，
可能會造成射頻擾動，在此種情況下，
使用者會被要求採取某些適當的對策。

CNS 15936:

警告：為避免電磁干擾，本產品不應安裝或使用於住宅環境。

IBM Taiwan Contact Information:

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Electromagnetic Interference (EMI) Statement - Korea

이 기기는 업무용(A급)으로 전자파적합등록을 한 기기이오니
판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의
지역에서 사용하는 것을 목적으로 합니다.

Germany Compliance Statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55032 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

EN 55032 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2014/30/EU) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 (0) 800 225 5423 or +49 (0) 180 331 3233
email: halloibm@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55032 Klasse A.

Electromagnetic Interference (EMI) Statement - Russia

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

User Interface

User Interface

The user interface is used to perform tasks on the Support Element console or on your system resources.

Note: A system that is IBM Dynamic Partition Manager (DPM) enabled can be managed only by using the user interface.

The user interface is comprised of several major components as shown in the following figure: the banner, the task bar, the navigation pane, the work pane, and the status bar.

The masthead, across the top of the workspace window, provides visual indicators of current overall system status, allows you to quickly find and open tasks; identifies the user name that you used to log in to; and includes easy access to your favorite tasks.

The navigation pane, in the left portion of the window, contains the primary navigation links for managing your system resources and the Support Element console. The links are referred to as *nodes*. Displayed above the navigation pane is the navigation toolbar.

The work pane, in the right portion of the window, displays information based on the current selection from the navigation pane or status bar. The contents of the work pane can vary depending on the type of systems you are managing through the SE. For example, when **Welcome** is selected from the navigation pane, the Welcome window content is displayed in the work pane.

You can resize the panes of the Support Element Console workspace by moving the mouse pointer over the border that separates the navigation pane from the work pane until the mouse pointer changes to a double-pointed arrow. When the pointer changes shape, press and hold the left mouse button that you drag the mouse pointer to the left or right. Release the button and your navigation pane or work pane is now larger or smaller in size.

The status bar, in the bottom left portion of the window, provides visual indicators of current overall system status. It also contains a status overview icon which may be selected to display more detailed status information in the work pane.

You can resize the panes of the Support Element console workplace by moving the mouse pointer over the border that separates the navigation pane from the work pane until the mouse pointer changes to a double-pointed arrow. When the pointer changes shape, press and hold the left mouse button while dragging the mouse pointer to the left or right. Release the button and your navigation pane or work pane is now larger or smaller in size. You can also do this within the System Management work pane border that separates the resources table from the tasks pad.

You can find more detailed help on the following:

Masthead

The SE masthead, which is located across the top of the workspace window, consists of the four major elements shown in Figure 7 on page 276.

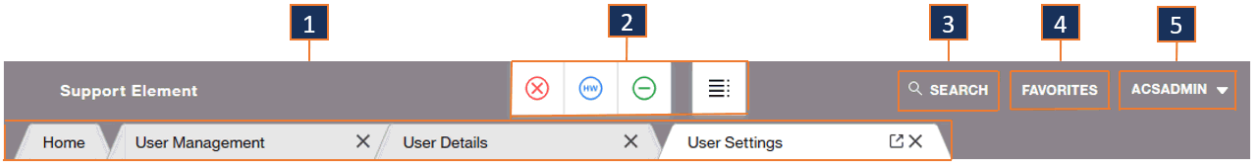


Figure 7. Elements of the SE masthead

1. Tabbed tasks:
   - The **Home** tab remains on the left of the masthead and displays the user interface for the console.
   - When a task opens, a new tab for that task is opened to the right of the **Home** tab.
   - You can close a task by selecting **X** on the tab.
   - You can open the task into a separate window by selecting the pop-out icon ( ). This capability allows you to view the task window in parallel on a single display, or you can move the task window to other physical displays. Then, you can return the task window back to the tabbed view by selecting the pop-in icon ( ).
   - Tabs of related tasks are grouped together. For example, in Figure 7 on page 276 , User Management and User Details are related so their tabs overlap.
2. Status icons provide visual indicators of current overall system status. It also contains a status overview icon, which you can select to display more detailed status information in the work pane.
3. **SEARCH** allows you to search for a task by name. Begin typing the task name in the input area. When the task name is displayed, select it to open the task in a new tab.
4. **FAVORITES** is a list of frequently used tasks that you create. Through **FAVORITES**, you can add a task to the list; edit the list by changing a task name; change the order in which the tasks appear, by using the up and down arrows next to the task name; and remove a task from the list.
5. The user name field displays the user name that you used to log in to the HMC. By clicking the drop-down arrow, you can perform the following tasks.
   - Open the **User Settings** task.
   - Access the **Help** for the user interface and expand the Table of contents to access all of the console help.

- Select **Logout** to open the **Logoff or Disconnect** task.

Navigation Pane

The SE navigation pane, which is located under the Home tab in the workspace window, contains the primary navigation links for managing your system resources and the Support Element Console. It also includes navigation methods that you can use when working with the user interface workspace. The primary navigation links, which are also called *nodes*, change the work pane display so you can manage your system resources or the SE, or access the list of all SE tasks. For more details click a topic link in the following list:

- Welcome
- System Management
- SE Management
- Service Management
- Tasks Index
- “Custom Groups” on page 288

It also includes the following navigation methods you can use when working with the user interface workplace:

Navigation Toolbar

The navigation toolbar, which is located above the navigation pane, consists of the following:

- To move forward and backward in the selection history for the work pane, use the forward and backward buttons.
- To return to the home page during your session and establish a home page to return to every time you log on to the console, use the home page and set home page buttons.
- To expand and collapse all of the nodes of the navigation pane, use the expand and collapse buttons.

You can point your mouse over the icon buttons to get a description of the function.

Navigation Pane Collapse and Expand Controls

The navigation pane collapse and expand controls are provided on the border between the navigation pane and the work pane. You can click these controls to collapse or expand the navigation pane that allows more work area in the work pane, if required. Hovering over these controls indicates whether you are hiding or displaying the navigation pane.

Welcome

Welcome work pane displays navigation information and the Support Element console version information.

To see the level of the Support Element console you are currently working with and other pertinent information, point your mouse over **SE Version** found at the top of the work pane.

System Management

System Management is used to manage and view system resources. Selecting the expand icon from the navigation pane displays a tree view of system resources that can include managed objects, as shown in Figure 8 on page 278.

Figure 8. Sample view of the expanded System Management node

Note: Not available when the system is IBM Dynamic Partition Manager enabled.

The **System Management** node represents all the resources that are managed by this Support Element console. When you select the **System Management** node from the navigation pane, all managed objects are displayed in the work pane, as shown in Figure 9 on page 278.

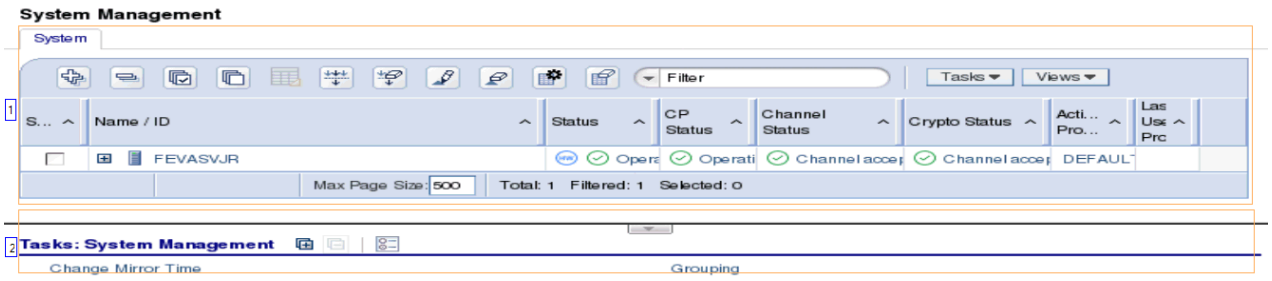


Figure 9. Sample System Management view in work pane

The Task Pad area of the work pane lists the tasks that you can select and open, based on the content of the selected **System Management** tab. The listed tasks can change when you make a selection in the tab display.

Note:

- You can use the collapse control, which is highlighted in Figure 9 on page 278, to hide the task pad.
- You can resize the areas within the Systems Management work pane by moving the mouse pointer over the border that separates the tab displays from the tasks pad. When the pointer changes shape, press and hold the left mouse button and drag the mouse pointer up or down. Release the button and the tab display or task pad is now larger or smaller in size.

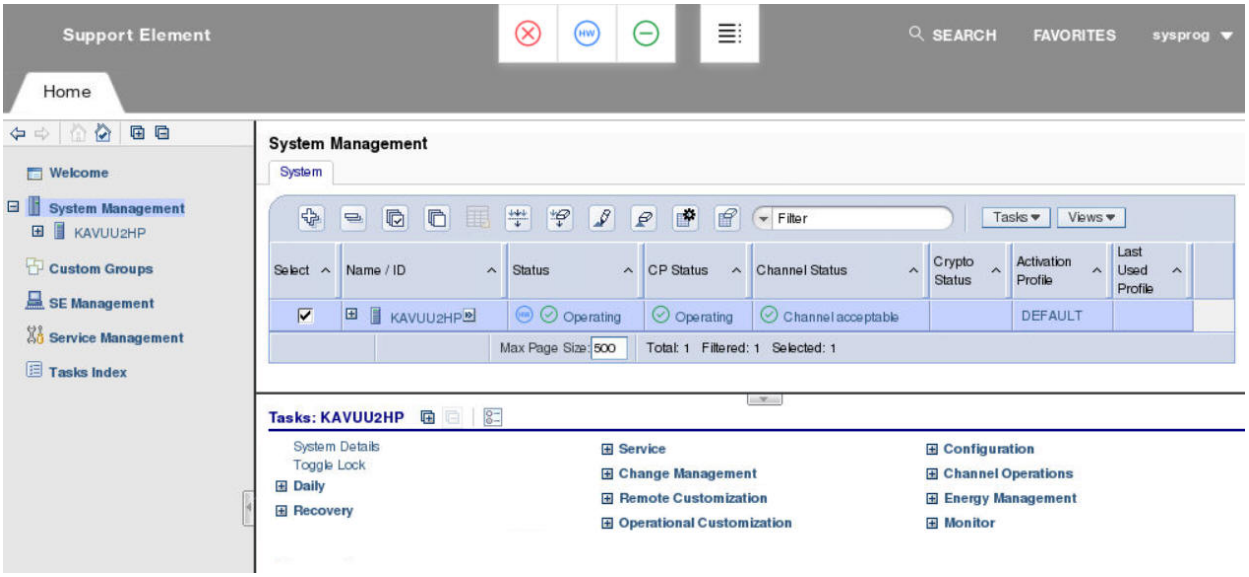
System

Note: The terms *system*, *server*, *object*, and *CPC* are used interchangeably.

The **System** node represents all the resources that are managed by this Support Element console.

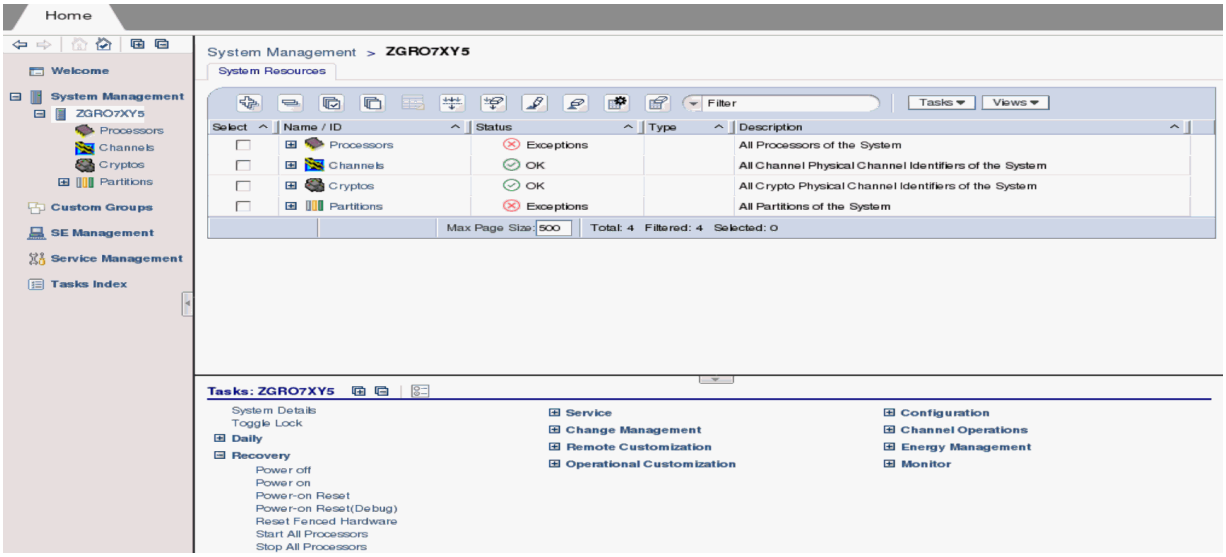
To work with the system:

- Select **System Management** from the navigation pane.
- Click in the **Select** column next to the system name in the work pane table.



When you select the **System** node from the navigation pane, a listing of individually defined objects is displayed under the **System** node in the navigation pane and the following resource tabs are displayed in the system work pane.

System Resources
Displays, in a table format, a list of all the managed system resources.



Note: Working with one system object at a time is the default, and is used in the examples throughout this Help information. However, if you want to work with more than one system object you can go to the **User Settings** task, select the **Controls** tab, deselect the **Single object selection** option, and click **Apply**. Now you can choose multiple system objects to manage.

Note: If a particular task cannot be performed on an object the task is not displayed.

You can find more detailed help on the following:

Opening tasks for the System

After you have chosen the systems to work with you are ready to perform tasks on them. The following task categories (groups) that are applicable to the systems you have chosen are displayed in the tasks pad. Task categories (groups) represent categories of tasks and are not tasks themselves. The available task group depends on the object selected from the navigation pane (System, Processors, Channels, Cryptos, Partitions). The following is the task groups that may be available for the system.

- Daily
- Recovery
- Service
- Change Management
- Remote Customization
- Operational Customization
- Object Definition
- Configuration
- Energy Management
- Monitor

You can select a task from these task groups in a variety of ways.

- Use the tasks pad below the systems work pane, see Tasks Pad.
- Click the context menu icon that appears next to the server name, see Context Menus.
- Click the **Tasks** menu from the work pane table toolbar, see Tasks Menu.
- Right-click in the cell containing the name of the object to display the context menu.

Note: If a particular task cannot be performed on an object the task is not displayed.

Tasks Pad

The Support Element console displays the tasks pad is displayed below the work pane table after you have selected the managed objects with which you want to work with.

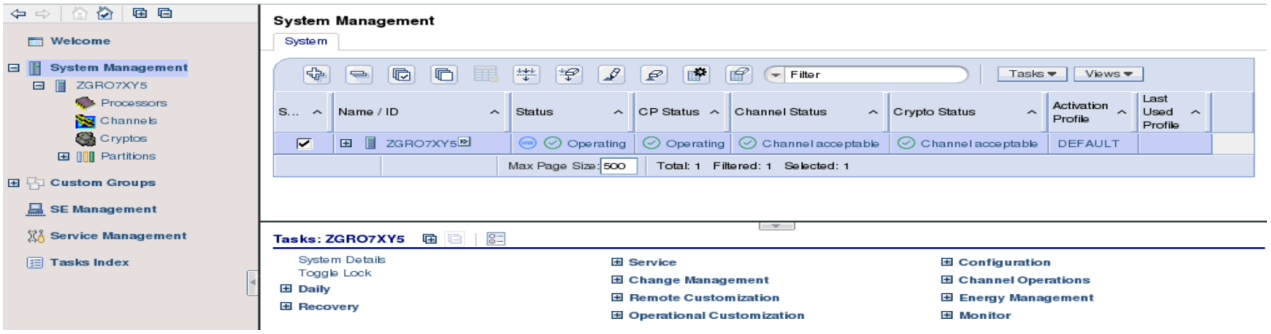
The following figure shows an example of tasks in the tasks pad that are available for the selected managed objects and applicable for the current user.

By default, the tasks pad is displayed. You can choose to hide the tasks pad by using the **User Settings** task.

To change the display of the tasks pad setting you can go to the **User Settings** task by selecting:

- **Task Index** or **SE Management** on the navigation pane, then open the **User Settings** task, or
- The user ID from the task bar to access the **User Settings** task to change the setting, or
- The **Close Tasks Pad** icon from the right side of the tasks pad title bar.

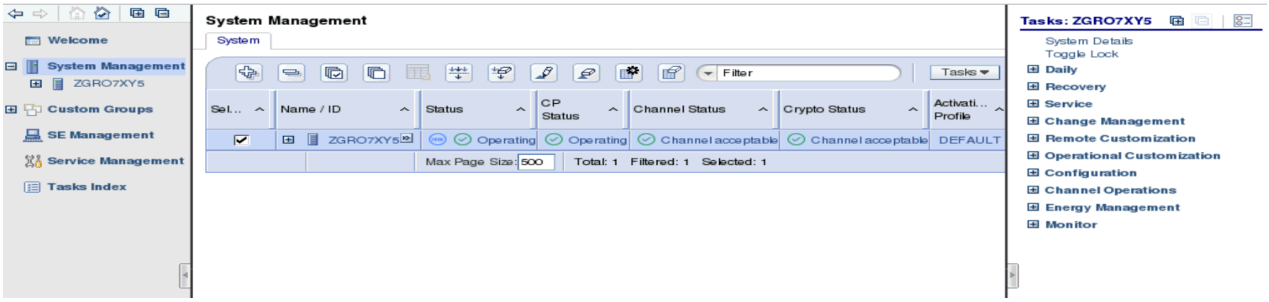
Note: To reset a closed tasks pad you must use the **User Settings** task.



Additional characteristics of using the tasks pad include:

- Resize the tasks pad by moving the mouse pointer over the border that separates the work pane table from the tasks pad.
- Use the collapse and expand controls icon that is provided on the border between the tasks pad and the work pane. You can click on these controls to collapse or expand the tasks pad allowing you more work area in the work pane, if required. Hovering over these controls indicates whether you will be hiding or displaying the tasks pad.
- Expand or collapse all the task groups in the tasks pad by selecting the **Expand All** icon or the **Collapse All** icon from the tasks pad title bar.
- Organize the tasks pad display by using the **Settings** icon from the tasks pad title bar. This option allows you to arrange the displayed tasks in a viewing format you prefer and in addition:
  - **Number of task columns** - Using the up and down arrows, select the number of columns you want displayed for the list of tasks.
  - **Expand task groups by default** - The task groups are expanded to display applicable tasks.
  - **Sort tasks alphabetically** - The tasks from all the task groups are sorted alphabetically.
  - **Position tasks pad vertically** - The tasks pad is rendered to the right of the work pane's table frame (see the following figure for an example).

    Note: When the tasks pad displays vertically the column count is not available.



This view displays the objects you selected from either the navigation pane tree or the work pane table view. Multiple objects are selected in the work pane table, therefore, the intersection of the selected objects' tasks are displayed.

If there are no objects selected in the work pane table, tasks are displayed in the tasks pad for the object selected in the navigation pane. Additionally, the tasks that display in the tasks pad are those available to the user currently logged in.

An example of using the tasks pad method:

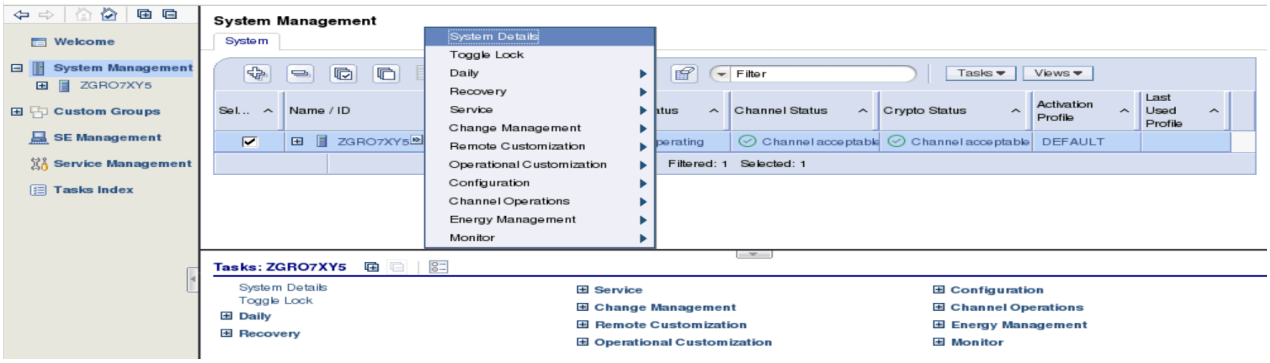
- Select the system in the work pane table (click in the **Select** column).
- Select a task group from the tasks pad (click the expand button or click the group name).

  Note: After you have expanded the task groups, those groups remain open so that you can repeatedly open other tasks without having to reopen the task groups again.
- From the task group, select the task that you want to perform.
- The initial task window is displayed.

Context Menus

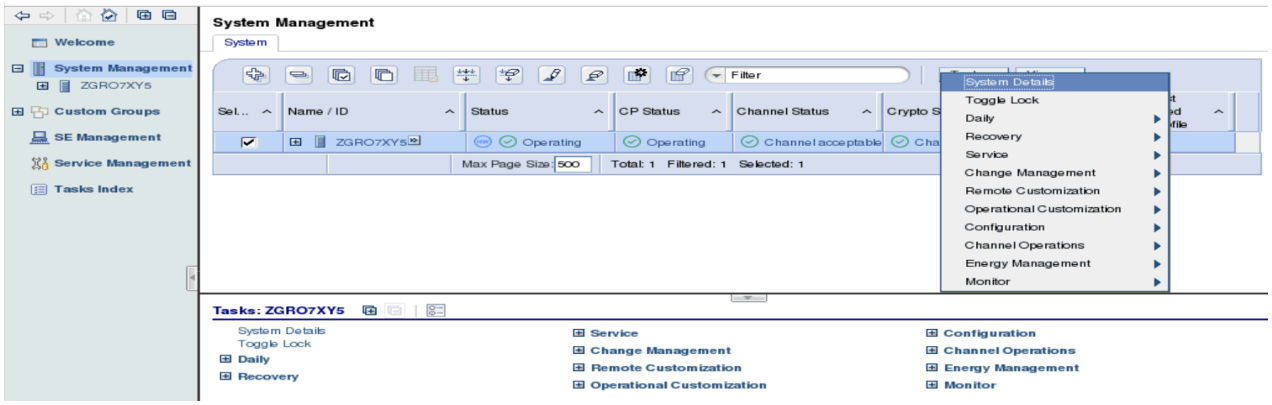
The context menu is a pop-up menu that lists the task groups associated with the selected object or objects. Context menus are only available for table selections. For example:

- Select the object or objects you want to work with in the **Select** column of the system work pane table. The context menu button (double right arrows) is displayed next to the object name you have selected.
- Click the button and the task groups menu is displayed for that particular object.
- You can also right click within the table cell of the object name to display the context menu.
- Select a task to open for the object. If more than one object is selected, the tasks that are displayed in the context menu apply to all selections.



Tasks Menu

The **Tasks** menu is displayed on the work pane table toolbar, as shown in the following figure. The tasks menu is only available for table selections. For example, in the **Select** column of the system work pane table, select the object you want to work with. Click **Tasks** for the list of the applicable task groups for the selected objects in the table. Select a task group, then select a task to open for the object. If more than one object is selected, the tasks that are displayed in the tasks menu apply to all selections.



Status

The **Status** column of the System work pane table displays the current status of the objects. If you select the status text, the help information for that status is displayed. Status icons can also be displayed in the status column next to the status text. Depending on the icon that is displayed, you can get the Hardware Messages task window or the Operating Systems Messages task window.

Displaying System Details

All system details can be displayed by using one of the following methods:

- Click the object name from the work pane table.
- Select the object name from the work pane table then:
  - Click **Details** from the tasks pad, or
  - Click the arrow icon next to the object name, then click **Details** from the context menu, or
  - Right-click in the object name table cell, then click **Details** from the context menu.

While you are in the **Details** window, you can also lock out disruptive tasks, or by clicking **Toggle Lock** in the tasks pad or from the context menu.

Note: Object locking cannot be applied to IBM Dynamic Partition Manager (DPM) objects.

The Systems Management work pane table includes additional information about the systems such as the activation profile name, last profile the server used, the machine type, and serial number of the server.

You can use the "Views Menu" on page 296 to customize the information that is displayed in the work pane table or the **Configure Columns** icon on the work pane table toolbar.

Processors

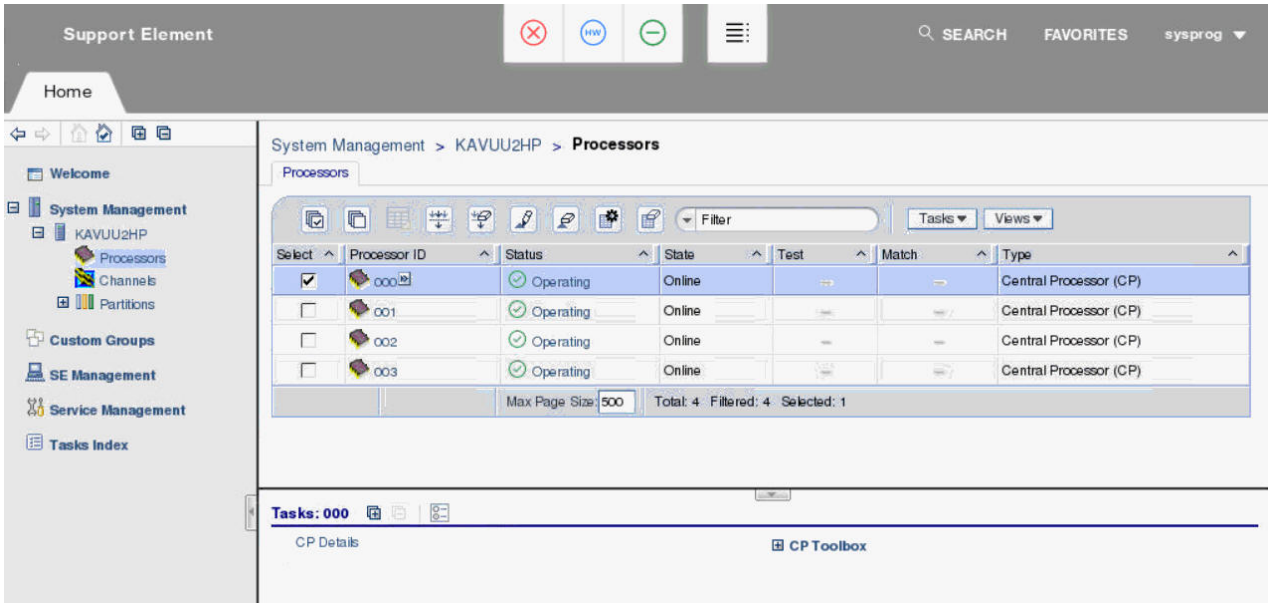
On the Support Element, both physical and logical processors are referred to as processors (CPs). When you select the **System** node from the navigation pane, the **Processors** node displays under the **System** node, as shown in the figure below. To work with the processors, select the **Processors** node in the navigation pane. A listing of processors is displayed in table view in the system work pane under the **Processors** tab. The default table identifies the ID, status, and state of each processors.

To display details about a partition from the Systems Management work pane table:

- Click the CP name from the **Name** column, or
- Click in the **Select** column next to the CP name to either:
  - Click **CP Details** in the tasks pad, or
  - Click the arrow icon next to the CP name and select **CP Details** from the context menu (see the following figure), or
  - Right-click the table cell of the CP name and select **CP Details** from the context menu.

In all cases, the **Details** window is displayed.

You can use the "Views Menu" on page 296 to customize the information that is displayed in the work pane table or the **Configure Columns** icon on the work pane table toolbar.

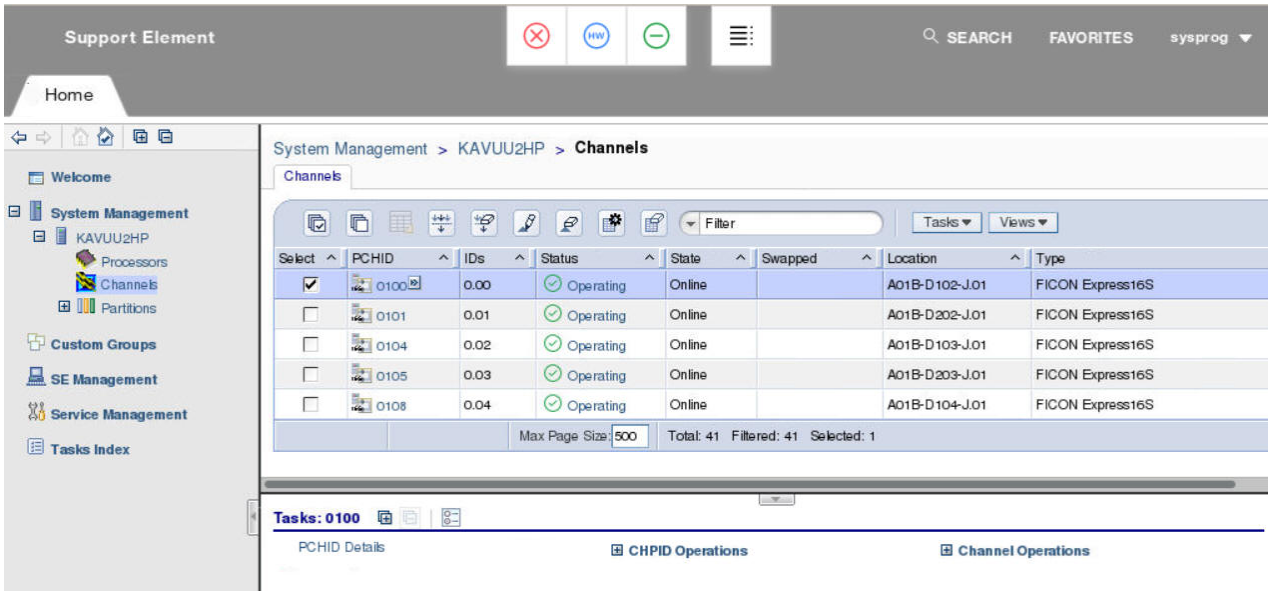


You can find more detailed help on the following:

Opening Tasks

Channels

The node that represents the system contains objects that represent all channels in the input/output (I/O) configuration. When you select the **System** node from the navigation pane, the **Channels** node displays under the system, as shown in the figure below. To work with the channels, select the **Channels** node in the navigation pane. A listing of channels is displayed in table view in the system work pane under the **Channels** tab. The default table identifies the physical channel identifier (PCHID), CSS.CHPID, status, state, cage-slot-jack address, and hardware type. Virtual channels will only be displayed after the system is activated.



To display details about a channel from the Systems Management work pane table:

- Click the channel name from the **Name** column, or
- Click in the **Select** column next to the channel name to either:

- Click **Image Details** in the tasks pad, or
- Click the arrow icon next to the partition name and select **PCHID Details** from the context menu (see the following figure), or
- Right-click the table cell of the partition name and select **PCHID Details** from the context menu.

In all cases, the **Details** window is displayed.

The Partitions work pane table includes additional information about the partitions such as the activation profile name, last profile the image used, the operating system name, type, and level for the partition.

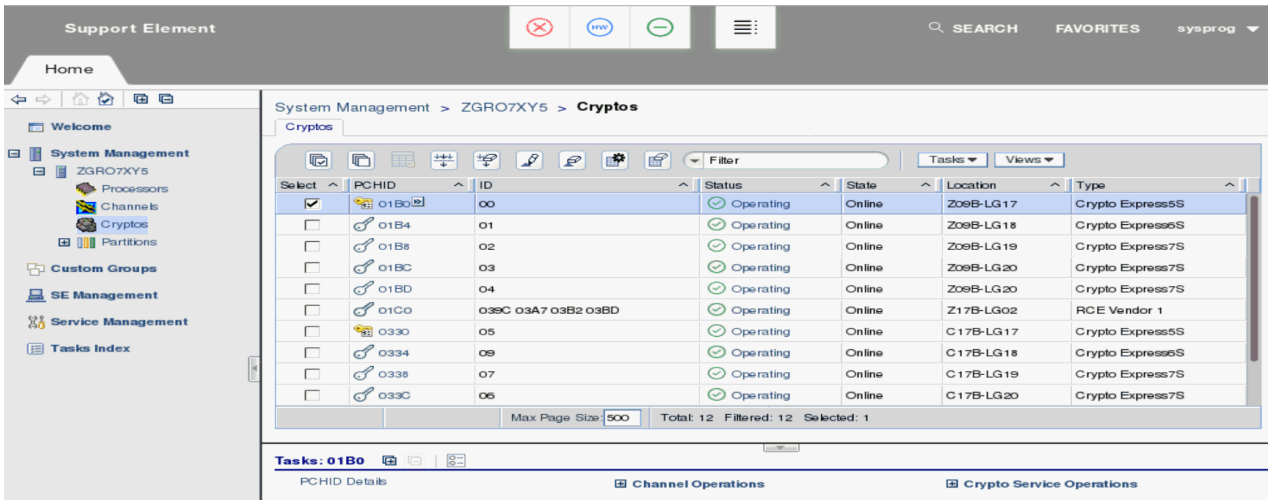
You can use the "Views Menu" on page 296 to customize the information that is displayed in the work pane table or the **Configure Columns** icon on the work pane table toolbar.

You can find more detailed help on the following:

Opening Tasks

Cryptos

The node that represents the system contains objects that represent all installed cryptos. When you select the **System** node from the navigation pane, the **Crypto** node displays under the system as shown in the figure below. To work with the crypto, select the **Crypto** node in the navigation pane. A listing of cryptos is displayed in table view in the system work pane under the **Cryptos** tab. The default table identifies the physical channel identifier (PCHID), crypto ID, status, state, cage-slot-jack address, and crypto type.



To display details about a crypto from the Systems Management work pane table:

- Click the crypto name from the **Name** column, or
- Click in the **Select** column next to the crypto name to either:
  - Click **PCHID Details** in the tasks pad, or
  - Click the arrow icon next to the crypto name and select **PCHID Details** from the context menu (see the following figure), or
  - Right-click the table cell of the crypto name and select **PCHID Details** from the context menu.

In all cases, the **Details** window is displayed.

The Partitions work pane table includes additional information about the partitions such as the activation profile name, last profile the image used, the operating system name, type, and level for the partition.

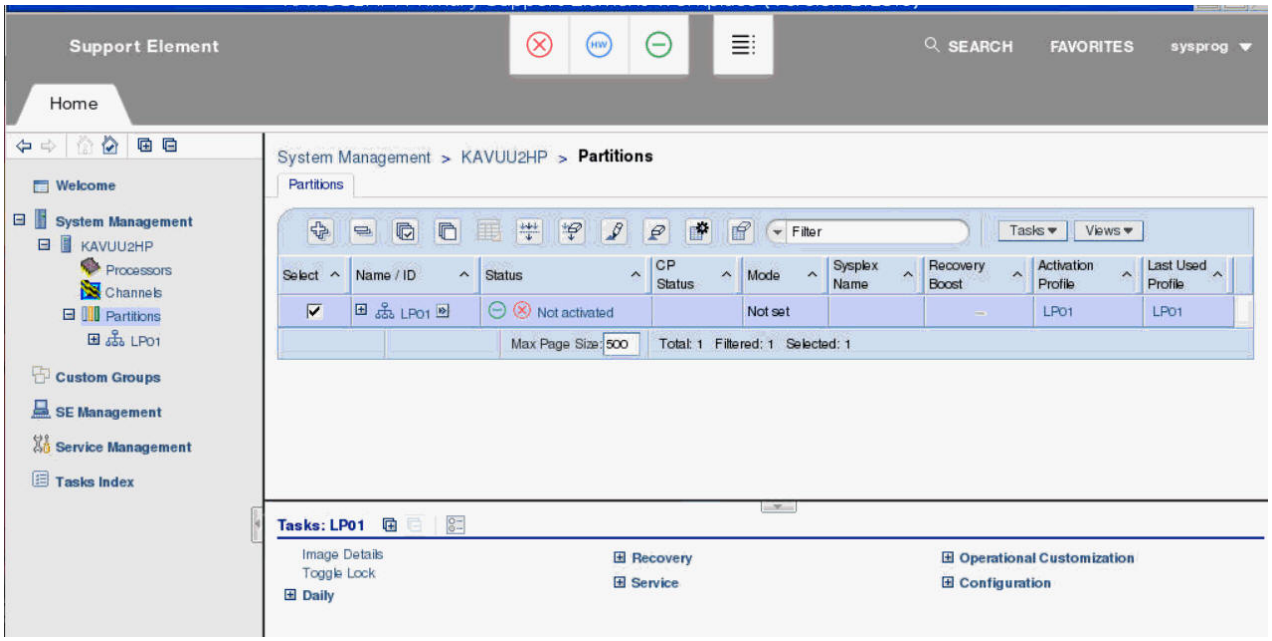
You can use the "Views Menu" on page 296 to customize the information that is displayed in the work pane table or the **Configure Columns** icon on the work pane table toolbar.

You can find more detailed help on the following:

Opening Tasks

Partitions

When the system is activated, the **Partitions** node contains objects that represent the logical partitions. Logical partitions are referred also as images. An image is a set of system resources capable of running a control program or operating system. When you click the **System** node from the navigation pane, the **Partitions** node displays under the system as shown in the figure below. To work with the partitions, select the **Partitions** node in the navigation pane. A listing of logical partitions is displayed in table view in the system work pane under the **Partitions** tab. The default table identifies the logical partition name, status, image mode, sysplex name, operating system name, activation profile, and last used profile.



To display details about an image from the Systems Management work pane table:

- Click the image name from the **Name** column, or
- Click in the **Select** column next to the image name to either:
  - Click **Image Details** in the tasks pad, or
  - Click the arrow icon next to the image name and select **Image Details** from the context menu (see the following figure), or
  - Right-click the table cell of the image name and select **Image Details** from the context menu.

In all cases, the **Details** window is displayed.

The Partitions work pane table includes additional information about the partitions such as the activation profile name, last profile the image used, the operating system name, type, and level for the partition.

You can use the "Views Menu" on page 296 to customize the information that is displayed in the work pane table or the **Configure Columns** icon on the work pane table toolbar.

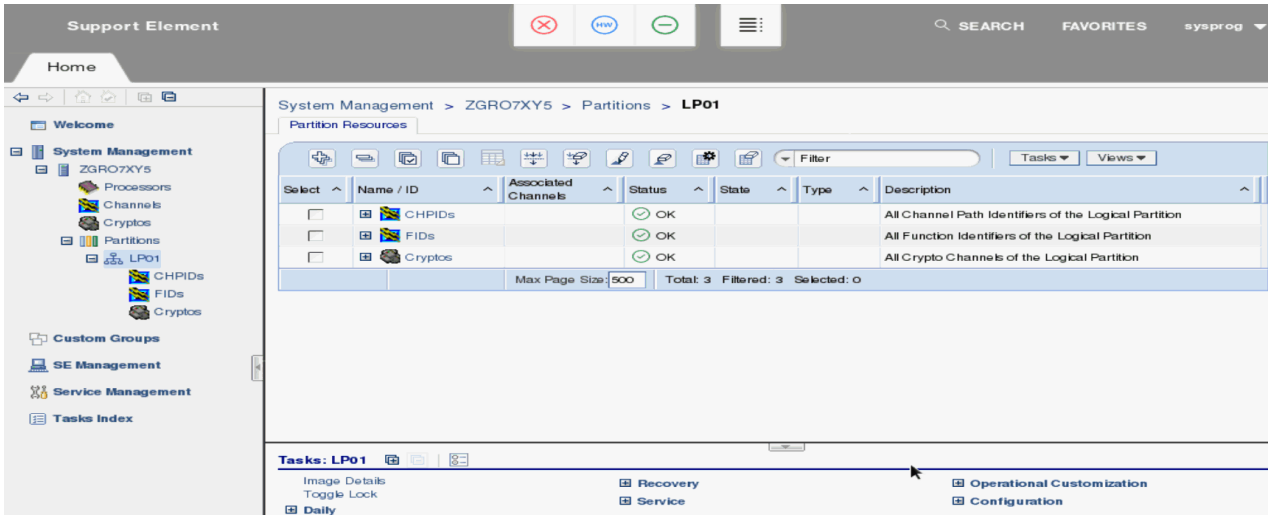
You can find more detailed help on the following:

Opening Tasks

Partitions Resources

When the system is activated, the **Partitions** node contains objects that represent the logical partitions. Logical partitions are referred also as images. An image is a set of system resources capable of running a control program or operating system. When you click the **System** node from the navigation pane, the **Partitions** node displays under the system node as shown in the figure below. To work with the partitions, select the **Partitions** node in the navigation pane then select a partition. The partition's defined resources display in the navigation pane below the selected partition and in table view in the work pane. The table identifies the resources defined in the partition. The resources can include CHPIDs, processors (CPs),

FIDs, and cryptos. Select the partition's defined resource from the navigation pane you want to work with. The defined resource displays information in table view in the work pane.



You can find more detailed help on the following:

Opening Tasks

System Management (Dynamic Partition Manager enabled)

System Management is used to manage and view resources for the system that is IBM Dynamic Partition Manager (DPM) enabled.

Note: The **System** node is referred to by the defined name of the system.

When you select **System Management** from the navigation pane, the following tabs can be displayed in the work pane (see the following figure):

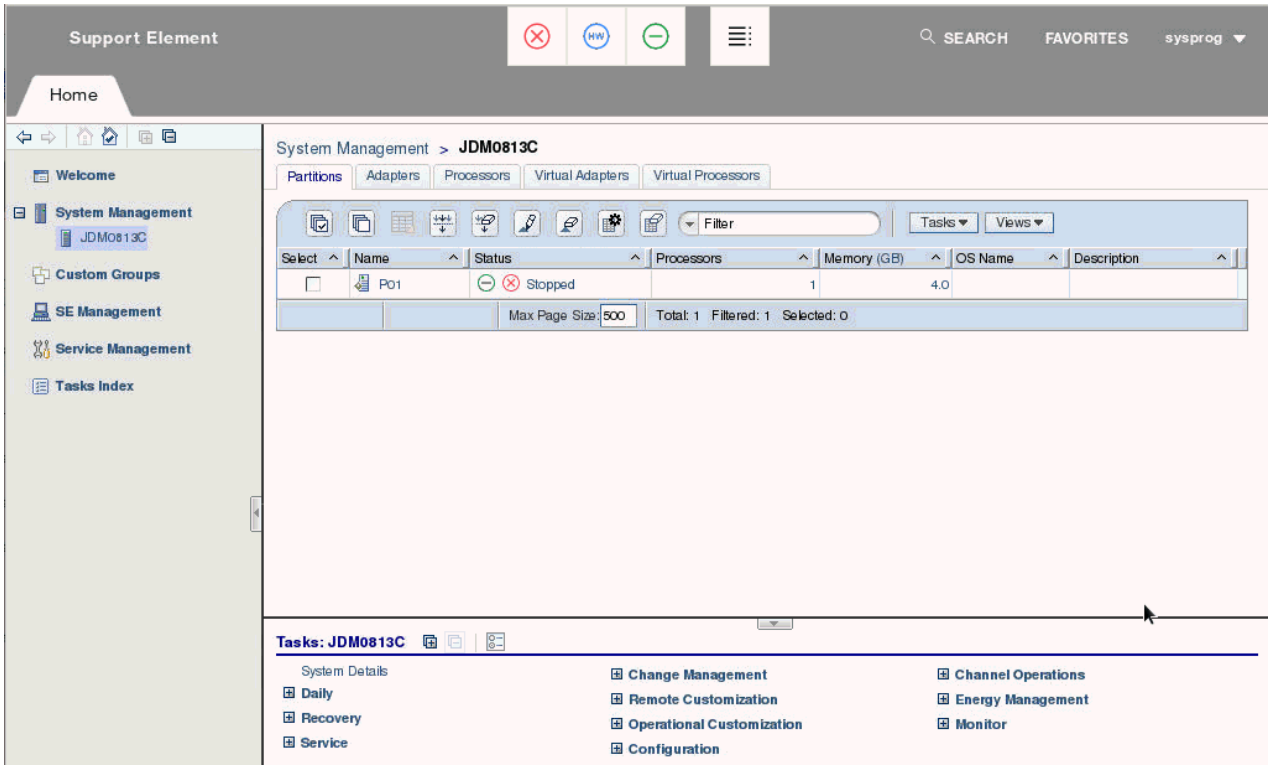


Figure 10. System Management - Dynamic Partition Manager enabled

System
Displays in table view the selected system that is Dynamic Partitions Manager enabled. The default table identifies the status, CP status, PCHID status, Crypto status, and description.

Partitions
Displays in table view the partitions for the system that is Dynamic Partition Manager enabled. The default identifies the status, processors, memory, operating system name, and description.

Adapters
Displays in table view the adapters for the system that is Dynamic Partition Manager enabled. The default identifies the ID, PCHID status, PCHID state, swapped, location, card type, and virtual adapter IDs.

Processors
Displays in table view the processors for the system that is Dynamic Partition Manager enabled. The default identifies the processor ID, status, state, test, match, and type.

Virtual Adapters
Displays in table view the virtual adapters for the system that is Dynamic Partition Manager enabled. The default identifies the virtual ID, adapter ID, partition, status, state, and type.

Virtual Processors
Displays in table view the virtual adapters for the system that is Dynamic Partition Manager enabled. The default identifies the virtual ID, adapter ID, partition, status, state, and type.

Custom Groups

The **Custom Groups** node provides a mechanism for you to group system resources together in a single view. In addition, groups may be nested to create custom "topologies" of system resources.

You perform tasks on objects in a group by selecting the group in the navigation pane and clicking on the check boxes in the **Select** column of the table. To perform tasks on all of those objects, click **Select All** from the table toolbar.

For group status information, status is displayed in the **Status** column in the work pane table. Status icons are displayed appropriately. If a group has both Hardware Messages and Operating System Messages, a message overlay icon is displayed indicating that both messages exist.

You can find more detailed help on the following:

User-Defined Groups

You can use the **Grouping** task under the Daily category from the tasks pad to create your own group that you want to work with. This task allows you to create new groups and manage existing ones. To create a group:

1. Select one or more objects that you want to include in the group.
2. Open the **Grouping** task from the **Daily** Tasks Pad. The **Manage Groups** window is displayed.
3. Select **Create a new group** from the **Manage Groups** window.
4. Specify a group name and description.
5. Click **OK** to complete.
6. The new user-defined group is displayed in the navigation pane under the **Custom Groups** node.

You can also create a group by using the pattern match method:

1. Without selecting an object you can open the **Grouping** task from the Custom Groups, System Management tasks pad, or Tasks Index.
2. From the **Create Pattern Match Group** window:
   - Select one or mode group types that you want to create.
   - Specify a group name, description, and the pattern used to determine if an object should be part of the group.
   - Click **OK** to complete.
3. The new user-defined group is displayed in the navigation pane under the **Custom Group** node.

   Note: Patterns specified in the **Managed Resource Pattern** input field are regular expressions. For example, if you specified **abc.***, all the resources that begin with **abc** will be included in that group.

SE Management

SE Management allows you to perform tasks associated with the management of this console. When you select **SE Management** from the navigation pane, the work pane contains a view of the Support Element console management tasks and their descriptions. These tasks are used for setting up the Support Element console and securing the Support Element console. Most likely, you will not use these actions on a regular basis.

To see what level of the Support Element you are currently working with, point your mouse over **SE Version** found at the top of the work pane.

To display the tasks in the work pane:

1. Select the **SE Management** node in the navigation pane.
2. From the work pane, click on the task you want to perform.
3. By default, a categorized listing of the tasks is displayed. The tasks are arranged in groups which include:
   - Configuration
   - Security.
4. From the work pane, click on the task you want to perform.

If you want an alphabetic listing of the task, go to the **View** drop-down menu, in the upper right corner of the work pane, and click **Alphabetical**. Click **Categorized** to go back to the task groups.

In addition, for each of the **Alphabetical** and **Categorized** views you can also choose a style of view:

- **Detail** displays a small task icon followed by the name and description in two columns.
- **Icon** displays large task icons above the task name.
- **Tile** displays tasks using large icons next to each task's name and description to help you find tasks by icon while still providing task descriptions.

Service Management

Service Management allows you to perform tasks associated with servicing the Support Element console. When you select **Service Management** from the navigation pane, the work pane contains a view of tasks and their descriptions. These tasks are used to service the Support Element console and maintain its internal code.

To see what level of the Support Element you are currently working with, point your mouse over **SE Version** found at the top of the work pane.

To display the tasks in the work pane:

1. Select the **Service Management** node in the navigation pane.
2. From the work pane, click on the task you want to perform.
3. By default, a categorized listing of the tasks is displayed. The tasks are arranged in groups which include:
   - Console Logs.
4. From the work pane, click the task you want to perform.

If you want an alphabetic listing of the tasks, go to the **View** drop-down menu, in the upper right corner of the work pane, and click **Alphabetical**. Click **Categorized** to go back to the task groups.

In addition, for each of the **Alphabetical** and **Categorized** sorts you can also choose a style of view:

- **Detail** displays a small task icon followed by the task name and description in two columns.
- **Icon** displays large task icons above the task name.
- **Tile** displays tasks using large icons next to each task's name and description to help you find tasks by icon while still providing task descriptions.

Tasks Index

Tasks Index performs tasks by allowing you to select them from the list. When you select **Tasks Index** from the navigation pane, the work pane contains an alphabetical listing of the tasks available for the user ID you are logged in as. For an example of the tasks index, see the following figure. You can open these tasks by clicking on the task name from the table. The table includes the following information:

Name
Names the task. The icon associated with the task can be hidden by disabling the work pane icons from the **User Settings** task.

Permitted Objects
Lists the category of objects that the task may be targeted to run against. The **SE Management** and **Service Management** tasks require no targets, therefore permitted objects are not specified.

You can filter on this column to display only the tasks permitted by particular objects. For example, if you want to display only the tasks that are acceptable on a partition, you can do the following:

1. Select the **Show Filter Row** icon. The filter row is displayed.
2. Click **Filter** that appears under **Permitted Objects**. The **Item** drop-down is displayed.
3. Click the drop-down arrow and select **Partitions**. Click **OK** to continue. A list of all tasks that apply to partitions is displayed.

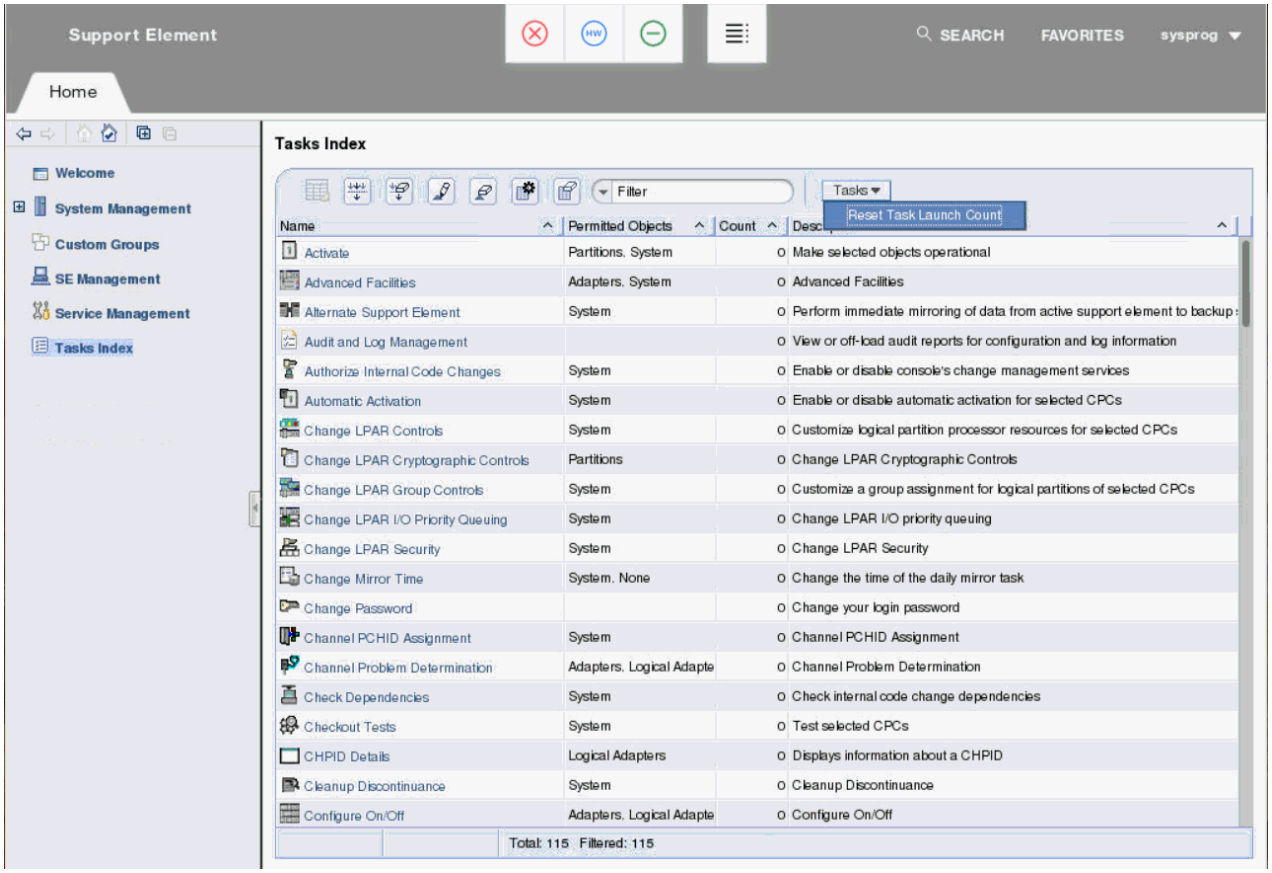
Count
Displays the number of times the task was opened by the current user.

Description
Describes the task.

Notes:

- If a task (for example, Activate) is applicable to one or more targeted objects, a secondary window is displayed for target selection.
- The **SE Management** and **Service Management** tasks are opened without prompting for targets.
- Each time you open a task, the count increments by one. The values in the **Count** column may be reset to zero by clicking **Tasks** from the work pane table toolbar, then selecting **Reset Task Launch Count** (see the following figure).
- You can use the work pane table toolbar icons for selecting, filtering, sorting, and arranging the information in the table. See Work Pane Table Toolbar for more detailed information about using the icons and the quick filter function.

- If a task (for example, Activate) is applicable to one or more targeted objects, a secondary window is displayed for target selection.
- The **SE Management** and **Service Management** tasks are opened without prompting for targets.
- Each time you open a task, the count increments by one. The values in the **Count** column may be reset to zero by clicking **Tasks** from the work pane table toolbar, then selecting **Reset Task Launch Count** (see the following figure).
- You can use the work pane table toolbar icons for selecting, filtering, sorting, and arranging the information in the table. See Work Pane Table Toolbar for more detailed information about using the icons and the quick filter function.



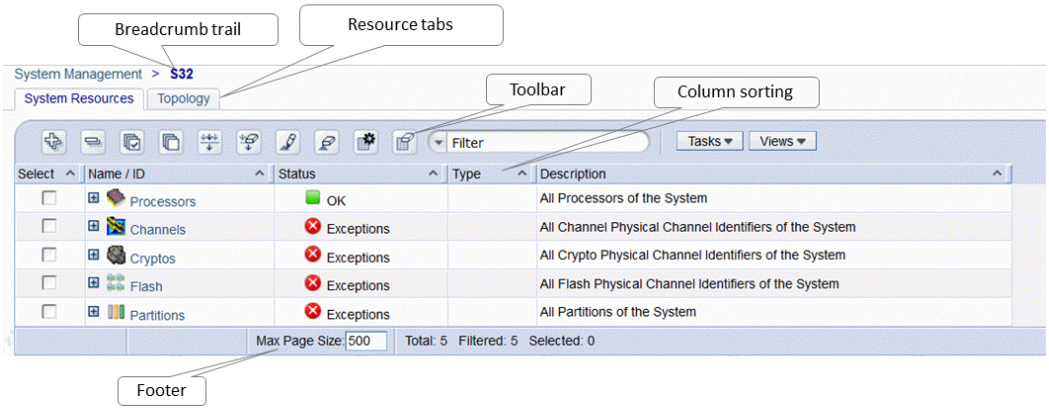
Work Pane

The work pane displays information based on the current selection from the navigation pane, resource tabs, or status bar.

The work pane described in this section discusses the functions of the **System Management** work pane.

Selecting an object from the navigation pane displays a resource (configurable) table in the work pane as shown in the following figure. This figure identifies some of the areas of the configurable table.

Note: You can click on the name of an object in the work pane table to display the **Details** window.



You can find more detailed help on the Work Pane table:

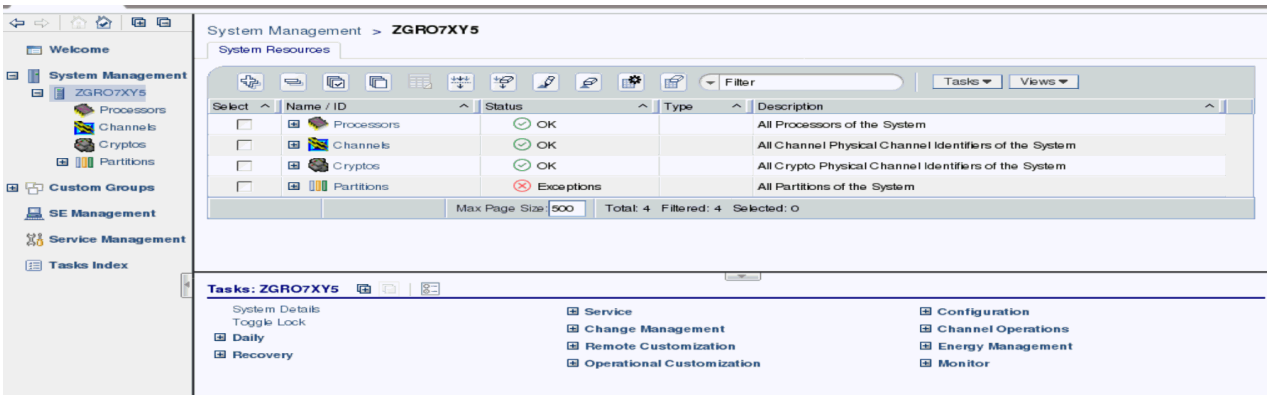
Work Pane Table

This information that is displayed in the work pane table allows you to view an object and its children in the same work pane table including its hierarchical relationships. Initially, all the objects of the navigation pane display a default predefined table view. These tables provide sorting, filtering, and column configuration of the data and allow for customization of which managed objects are displayed in which order. See Work Pane Table Toolbar for customization of the managed objects.

If an object in the **Name** column contains additional objects, an icon to expand (+) or collapse (-) the item is displayed before the object name. This allows you to view all the additional objects within the object. You can continue to perform tasks on the expanded objects. As you place the cursor over the icon, help information is displayed. This information describes the function of the icon. If you have been sorting or filtering in the work pane table, the help information indicates that you are unable to expand or collapse the object.

You can customize these tables using the **Manage Views** option from the **Views** menu, see Creating a Custom Work Pane Table View.

For an example of the work pane table view, see the following figure.



You can also reorder the columns of the table view work pane table by using the drag and drop method:

1. Place the cursor on the heading of the column you want to move. You will see the cursor change to a cross hair indicating it can be moved.

   Note: The **Select** and **Name** columns are the only columns that cannot be moved.
2. Hold down the left mouse button and drag the column to the desired placement in the table. You cannot drag a column past the **Name** column.
3. The column settings are saved for you. If you want to go back to the original column settings, click the **Reset Column Order, Visibility, and Widths** icon.

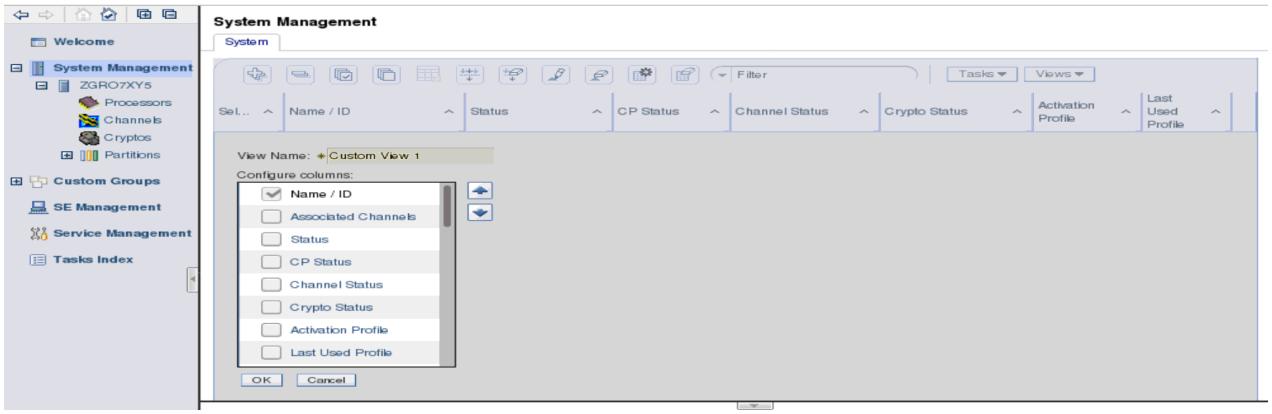
You can find more detailed help on the following.

Creating a Custom Work Pane Table View

The columns that are available when you create customized views are an aggregate of its default table columns and the default table columns of all children. You can create your own user-defined column sets by selecting the **Manage Views** option from **Views** the menu.

If you are creating a new table view for the first time, perform the following steps:

1. Select the **Manage Views** option from the toolbar's **Views** menu.
2. Click **New** from the **Manage Views Dialog** that displayed above the resources table
3. You can specify a unique name for your custom view in the **View Name:** input field. (see the following figure).
4. Select the items and order from the **Configure columns:** list you want included in your view. Use the arrows to manage the order of the columns. Note that **Name** cannot be moved or hidden in the column configuration.
5. Click **OK** when you have completed the customization of your view. The new table view that you created is displayed when you select the **Views** menu.



Renaming a Custom Work Pane Table View

To rename a work pane table view, perform the following steps:

1. Select the **Manage Views** option from the toolbar's **Views** menu.
2. Select the custom table view name that you want to rename from the **Custom Table Views** list.
3. Click **Rename** in the **Manage Views Dialog**.
4. Specify a unique name for the selected custom table view name.
5. Click **OK** to save your new custom table view name.
6. The new name will appear in the **View** menu.

Deleting a Custom Work Pane Table View

To delete a work pane table view, perform the following steps:

1. Select the **Manage Views** option from the toolbar's **Views** menu.

2. Select the custom table view name that you want to rename from the **Custom Table Views** list.
3. Click **Delete** in the **Manage Views Dialog**.
4. If a confirmation panel displays, click **OK** to confirm the deletion.
5. The selected name is not displayed in the **Views** menu.

Changing a Custom Work Pane Table View

The columns that are available when you create customized views are an aggregate of its default table columns and the default table columns of all children. To load the selected custom view and configure the columns in the table view, perform the following steps:

1. Select the **Manage Views** option from the toolbar's **Views** menu.
2. Select the custom table view name that you want to configure from the **Custom Table Views** list.
3. Click **Configure** in the **Manage Views Dialog**.
4. Change column selections and column order.
5. Click **OK** to save your changes.
6. The table is displayed as specified by your selections.

Work Pane Title and Breadcrumb Trail

The work pane title is displayed directly above the work pane table resource tabs. It identifies the System Management group. Once you begin drilling down to more specific objects from the navigation pane, a breadcrumb trail is displayed on the work pane title line. These breadcrumbs identify the navigation path that led you to the current work pane resources table. You can use the links from the navigation path to go to the previous pages. The resource tabs that are displayed in the work pane depends on the resource selected from the navigation pane.

Work Pane Table Footer

The table footer located at the bottom of the work pane table includes information about the number of pages of information included for the displayed table. It also displays additional summary information such as the number of items selected in the work pane table, filtered total, or the row count of the number of rows displayed in the current page.

You can change the number of items you want displayed on each page of the table by specifying a number in the **Max Page Size** input field, then press Enter. If more than one page of information is available a page count is displayed and you have the ability to go to a page directly by specifying a page number in the entry field, then press Enter.

Work Pane Table Toolbar

The toolbar at the top of the System Management work pane all resources table contains icons used to expand, collapse, select, filter, sort, and arrange the entries in the resources table. Hovering over the toolbar buttons displays their functions. The toolbar also includes **Tasks** and **Views** menus that can be used with the information displayed in the resources tables.

You can find more detailed help on the work pane views:

Expanding and Collapsing Resources

The **Expand All** icon allows you to list all the resource groups. The **Collapse All** icon allows you to collapse all the resource groups. These icons work on all those objects that have additional objects associated with them in the table.

Note: These icons are disabled if you are sorting, filtering, or quick filtering. In addition, the table hierarchy is removed.

Selecting Rows

You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block. Click **Select All** or **Deselect All** to select or deselect all objects in the table. The table summary at the bottom of the table (work pane table footer) includes the total number of items that are selected. To set the object selection mode use the **User Settings** task.

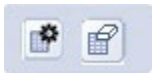
Filtering

If you click **Show Filter Row**, a row is located under the title row of the table. Click **Filter** under a column heading to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the check box next to the desired filter in the filter row. Click **Clear all Filters** to return to the complete listing. The table summary includes the total number of items that pass the filter criteria and the total number of items.

Sorting

Edit Sort and **Clear All Sorts** perform multicolumn sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, you can perform single column sorting by selecting the **^** in the column header to change from ascending to descending order. Click **Clear All Sorts** to return to the default ordering.

Column Configuration



Use the column configuration buttons to manage the columns displayed in the System Management tree view. Click **Configure Columns** to arrange the columns in the table in the order you want or to hide columns from view. All available columns are listed in the Columns list by their column names. You select the columns you want displayed or hidden by selecting or clearing the box next to the column names. Manipulate the column order by selecting a column name in the list box and clicking the arrow buttons to the right of the list to change the order of the selected columns. When you have completed the configuration of the columns, click **OK**. The columns are displayed in the table as you specified. If you want to go back to the original layout of the table, click **Reset Column Order, Visibility, and Widths** on the table toolbar. Select one or more of the properties to reset to their original layout, and click **OK**.

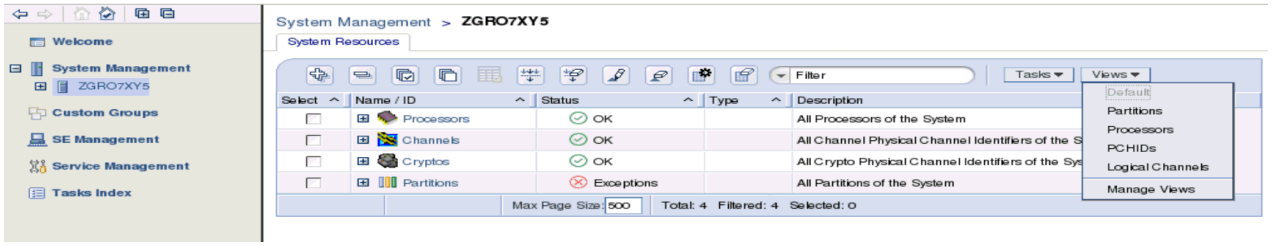
Quick Filter

Use the quick filter function to enter a filter string in the Filter input field, and then press **Enter** to apply the filter. By default all the columns are filtered, showing only rows containing a cell whose value includes the filter text. Clicking the arrow displays a menu that restricts the columns to which the filter is applied.

Views Menu

The **Views** menu is displayed on the work pane table toolbar when working with managed objects and custom groups. Use this menu to display different sets of attributes (columns) in the table. The following figure shows an example of the **Views** options when you are working with the system.

For information on defining your own table or tree views, see Creating a Custom Work Pane Table View.



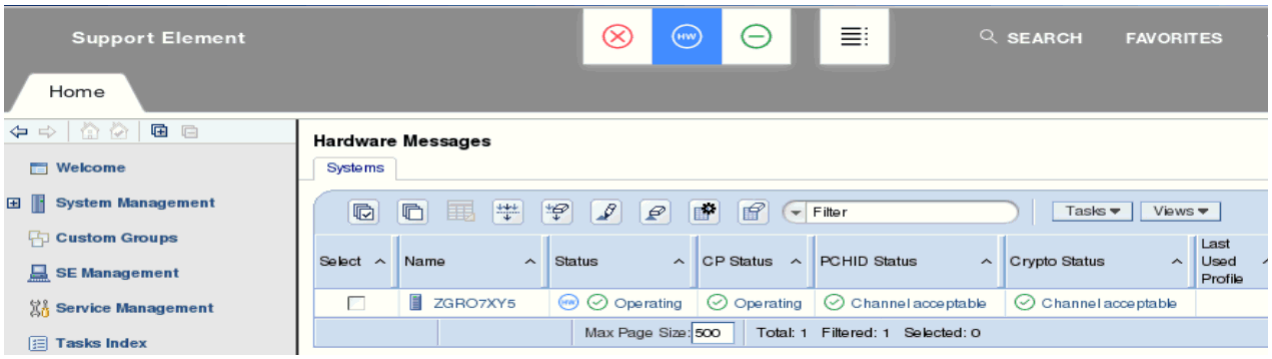
The following figure shows an example of the **Views** options when you are working with user-defined custom groups.

Status Bar

The status bar, located in the masthead, provides an "at a glance" view of the indicators (icons) for exceptions, hardware messages, operating system messages, and overall system status. When no objects exist with a given status icon, then the icons are green to convey a positive status.

When objects exist with a status icon other than green they are represented by red for exceptions, blue for hardware messages, and purple for operating system messages. Icons are displayed in the work pane table next to a managed object when it is in an Exception State or when it receives a hardware or operating system message.

Click any of the individual icons in the status bar to view a listing of resources. For example, select the **Hardware Messages** icon to view all resources with a hardware message state in the work pane, as shown in the following figure.



You can find more detailed help on the following elements of the status bar:

Exceptions

If any managed object is in unacceptable state, the Exceptions indicator (icon) is displayed on the status bar. When you select the **Exceptions** indicator (icon) it displays a table in the work pane of only the objects in an unacceptable state.

Hardware Messages

If a managed object receives a Hardware Message, the Hardware Message indicator (icon) is displayed on the status bar. When you select the **Hardware Messages** icon it displays a table in the work pane of only the objects with hardware messages. The table includes the object name, status, and description. To view the hardware message for a particular object you can click on the Hardware Message icon in the **Status** column or you can select the object by clicking in the **Select** column next to the object name(s), click **Daily** in the tasks pad, and click **Hardware Messages**. The **Hardware Messages** window is displayed. Now you can work with it's messages.

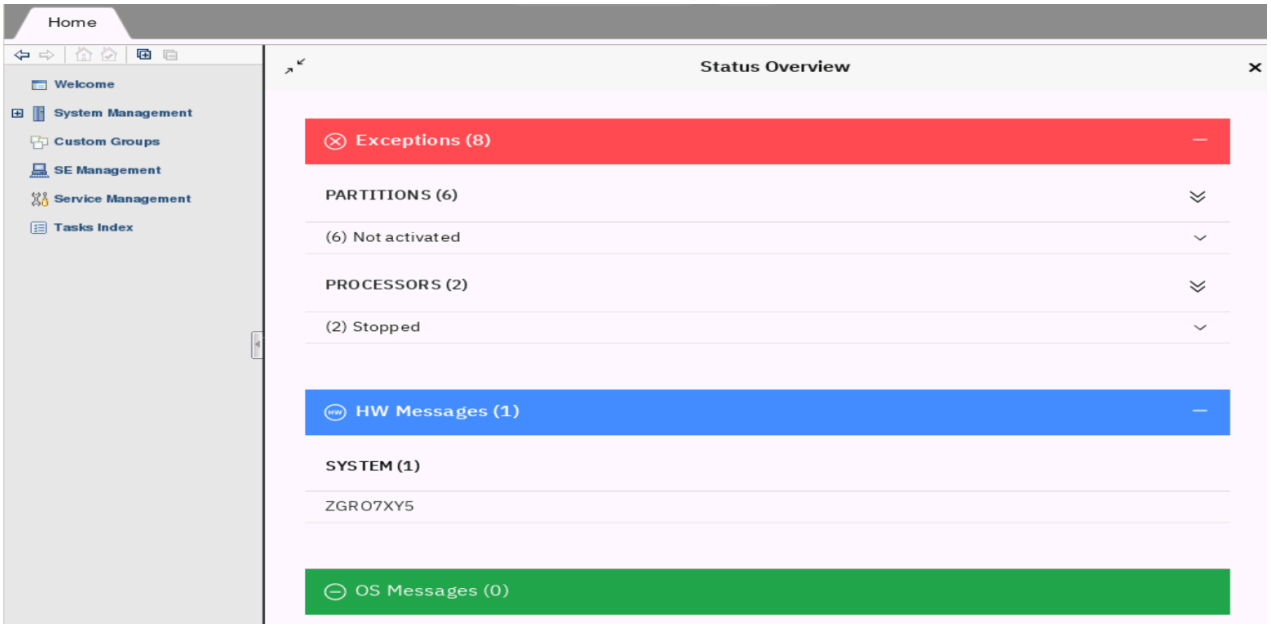
Operating System Messages

If a managed object receives an operating system message, the Operating System Message indicator (icon) is displayed on the Status Bar. When you select the Operating System Messages indicator (icon) it displays only objects with unviewed operating system messages requiring attention. The table includes the object name, status, and description. To view the operating system messages for a particular object you can click on the Operating System Messages icon in the **Status** column or you can select the object by clicking in the **Select** column next to the object name(s), click **Daily** in the tasks pad, and click **Operating System Messages**. The **Operating System Messages** window is displayed. Now you can work with your messages.

Status Overview

When you select the **Status Overview** icon, it displays a more detailed view of overall status in the work pane. It summarizes the total number of exceptions, hardware messages, and operating system messages by objects. Then, you can select a link from the work pane to display all objects with the particular state in the work pane. Following are some examples of the Status Overview function.

If you select the **Status Overview** icon when the Home tab is selected, the Status Overview is expanded in the work area, as shown in the following example.



If you select **Exceptions**, **HW Messages**, or **OS Messages**, content that is applicable for each appears as it would if you selected the icons form the Status Bar in the masthead area. If you select the plus sign (+) for each, the content is expanded with more detailed information.

You can use these additional icons from the **Status Overview** area:

Expand or Collapse All

Select this icon to view (expand) all the objects in an unacceptable state. You can select it again to hide (collapse) all the objects.

Expand or Collapse

Select this icon to view (expand) the objects for that specific unacceptable state. You can select it again to hide (collapse) the objects for that specific unacceptable state.

View message

Select this icon to view the hardware messages and operating system messages that are associated with the particular system.

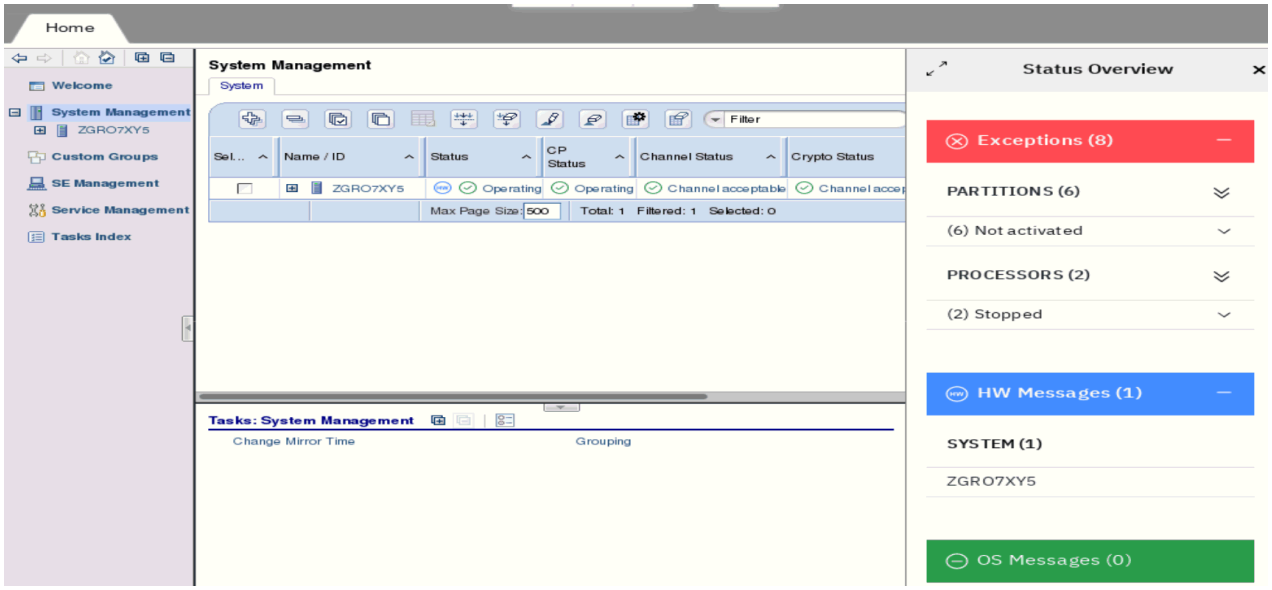
Status Overview - Close

Select this icon to close the Status Overview area.

Collapse or Expand Status Overview

Select this icon to collapse the Status Overview area where it appears along the right side of the user interface, as seen in the following example. You can select it again to make it viewable (expand) again in the work pane.

Note: When the Status Overview is collapsed, it is always visible whether the Home tab or a task tab is selected.



Object Locking for Disruptive Tasks

You can tell when the system or the system object is locked because a small lock icon is displayed next to the system or system object name in the work pane. In the topology view the icon is displayed as an overlay of the object icon.

Note: Object locking cannot be applied to IBM Dynamic Partition Manager (DPM) objects.

The setting of the system or the system object's toggle lock determines whether you can perform a disruptive task on the system or the system objects. You can lock an individual object or automatically lock all objects.

To individually lock (or unlock) the system or a system object:

1. Select the system from the table that you want to lock (or unlock).
2. Click **System Details** from the **Tasks Pad**, the **System Details** window is displayed.
3. You can select **Yes** or **No** for **Lock out disruptive tasks**.
4. Click **Apply** to make the change.

   There is also an automatic way to lock the system and all the system objects that are displayed on the workplace at one time. Unlike the previous ways for locking an object, using this method can cause the object to be relocked automatically if it was unlocked to perform a task on it. To use this method, you must have a user ID with the predefined user roles of an *Advanced Operator, System Programmer, Access Administrator*, or *Service Representative* for the Support Element console.

   a. Open the **Object Locking Settings** task from the **SE Management** Work Pane. The **Locking** window is displayed.

   b. Select **Automatically lock all managed objects** or **Relock after a task has been run** or both.

   If you need to unlock an object or a group of objects, you must unlock each one individually.

Tasks

SE Tasks

You can use the Table of Contents for more information on the Support Element (SE) tasks.

Activate

Accessing the Activate task for the CPC

Note: This task is not available when one or more managed systems have DPM enabled.

Use the Support Element workplace to start the task for activating the central processor complex (CPC).

Note: Activating a CPC can be considered disruptive. If the CPC is locked, unlock it.

To activate the CPC:

1. The CPC must have access to the input/output configuration data set (IOCDS) and operating systems referred to in the reset profile. See "Preparing an IOCDS".
2. Locate the CPC to work with.
3. Locate and open the **Activate** task.
4. Review the information on the Activate Task Confirmation window to verify the object you will activate is the CPC, and the activation profile it will use is the one you want.
5. If the information is correct, click **Yes** to perform the activation.

   The Activate Progress window indicates the progress of the activation, and the outcome.
6. Click **OK** to close the window when the activation completes successfully.

   Otherwise, if the activation does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

After the CPC is activated, you can use the **Activate** task again, if necessary, to selectively activate its images.

Accessing the Activate task for an object

Note: This task is not available when one or more managed systems have DPM enabled.

Use the Support Element workplace to start the task for activating an object and if they support activation profiles, the activation profiles to be used for each object of the central processor complex (CPC).

An *image* is a set of CPC resources capable of running a control program or operating system. One or more images is created during a power-on reset of a CPC. Each logical partition is an image.

To activate an object:

1. You must activate the CPC, and the activation must complete with at least a successful power-on reset of the CPC.
2. If you are activating an image, you must customize an activation profile and assign it to the image.
3. The system must have access to the operating system referred to in the activation profile.
4. Locate the object. If the object is an image, locate the image to which you assigned the activation profile.

   Note: Activating an object can be considered disruptive. If the image is locked, unlock it.
5. Locate and open the **Activate** task.
6. Review the information on the Activate Task Confirmation window to verify the object or image you will activate is the image, and the activation profile it will use is the one you want.
7. If the information is correct, Click **Yes** to perform the activation.

This displays the Activate Progress window. The window indicates the progress of the activation, and the outcome.

8. Click **OK** to close the window when the activation completes successfully.

   Otherwise, if the activation does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

Activate Task Confirmation

Note: This task is not available when one or more managed systems have DPM enabled.

Use this window to verify the objects and if they support activation profiles, the activation profiles to be used for each object.

Profile information for each object that supports profiles can be obtained by selecting an object and clicking **View Details...**.

Activate Table

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears. The icons perform the following functions:

Show Filter Row
If you select the **Show Filter Row** button a row is displayed under the title row of the table. Select Filter under a column to define a filter for that column to limit the entries in a table. Tables can be filtered to show only those entries most important to you. The filtered view can be toggled on and off by selecting the check box next to the desired filter in the filter row.

Clear All Filters
Select the **Clear All Filters** button to return to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
The **Edit Sort** button is used to perform multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, single column sorting can be performed by selecting the ^ in the column header to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Following are descriptions for the columns displayed in the Activate table:

Object Name
Displays the names of the objects that have been selected for the **Activate** task.

Type
Displays the processing environment of the selected objects.

Activation Profile
Displays the profiles for the selected objects.

Last Used Profile
Displays the name of the last profile used by **Activate**. If no previous profile has been used, the message "Not set via Activate" appears in place of a profile name.

Confirmation Text
Displays additional information about the selected object.

You can choose the following actions from this window:

Yes
To activate the selected object(s), click **Yes**.

No
To cancel your request to activate this object, click **No**.

View Details...
To display the values of the profile settings, click **View Details...**.

Help
To display help for the current window, click **Help**.

Activation Profiles List

Customize/Delete or View Activation Profiles List

Use this window to view, change, create, and delete activation profiles for the selected objects.

List of profiles for *object-name*
Lists the activation profiles for the CPC or image selected.

The toolbar at the top of the Overview table contains icons used to select, filter, sort, and arrange the columns in the Overview table.

You can work with the table by using the table icons or **Select Action** list from the table tool bar. Filter the data you would like to appear in the Overview table by manipulating the information in the table. If you place your cursor over an icon, the icon description appears.

The icons perform the following functions:

Select All
The **Select All** icon allows you to select all the objects in the Overview table.

Deselect All
The **Deselect All** icon allows you to deselect all the objects in the Overview table.

Show Filter Row
The **Show Filter Row** icon allows you to define a filter for a table column to limit the entries in a table. Tables can be filtered to show only those entries most important to you. The filtered view can be toggled on and off by selecting the check box next to the desired filter in the filter row.

Clear All Filters
The **Clear All Filters** icon allows you to return to the complete table summary. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
The **Edit Sort** icon allows you to perform multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, single column sorting can be performed by selecting the ^ in the column header to change from ascending to descending order.

Clear All Sorts
The **Clear All Sorts** icon allows you to return to the default ordering.

Configure Columns
The **Configure Columns** icon allows you to arrange the columns in the table in the order you want or to hide columns from view. All available columns are listed in the Columns list by their column names. You select the columns you want displayed or hidden by selecting or clearing the box next to the column names. Manipulate the column order by selecting a column name in the list and clicking the arrows to the right of the list to change the order of the selected columns.

Select one Profile Name from the list, then click on the task you want to perform.

Profile Name
Displays the name of the profile.

Type
Identifies the general contents and use of the profile.

Profile Description
Displays additional information about the profile, such as its specific contents or use.

Note: A description is an optional profile parameter; some profiles may not have one. When you customize the profile you can provide or omit its description.

Additional information is available from this window:

New image profile (Customize/Delete only)
To display the new image profile wizard to guide you through the process of creating a new image profile for the selected new image profile, click **New image profile**.

Customize profile (Customize/Delete only)
To select a reset, load, image, group, or list of image profiles that will allow you to modify certain parameters and then be applied to those selected profiles, click **Customize profile**.

Notes:

- If two or more profiles are selected and they are not all image profiles, **Customize profile** is grayed out.
- If an IOCDS **D0** image profile is selected, this image profile displays in view only.

Delete (Customize/Delete only)
To erase the selected activation profile, click **Delete**.

Notes:

- You cannot delete the activation profiles named **DEFAULT** and **DEFAULTLOAD**.
- When you click **Delete** to delete the selected activation profile, you will delete the profile for the object on the current window only.

  Deleting the selected activation profile will *not* affect profiles with the same name for other objects in other windows.

View (View only)
To view the current information and settings of the selected activation profile for the CPC, click **View**.

Close
To close the window when you are finished working with activation profiles for the selected object, click **Close**.

Closing the window does *not* affect any profiles you deleted.

Help
To display help for the current window, click **Help**.

View LPAR Weights

Use the View LPAR Weights window to check the partitions initial processing weights for the selected active IOCDS. You can use the drop-down menu to select a different IOCDS.

An initial processing weight represents the share of resources guaranteed to a logical partition when all processor resources are in use. Otherwise, when excess processor resources are available, the logical partition can use them if necessary. When a logical partition is not using its share of processor resources, other active logical partitions can use them. The exact percentage of resources allocated to the logical partition depends on the processing weights of other logical partitions defined and activated on the central processor complex (CPC) at the same time.

Image Name
Specifies the name of the partitions assigned to the selected IOCDS.

Processor Type
Specifies the processor types for each partition in the selected ICODS.

Initial Weight
Specifies the relative amount of shared processor resources assigned to each partition.

Additional functions on this window include:

Close
To close this window, click **Close**.

Help
To display help for the current window, click **Help**.

Change Object Options

Use this window to assign a profile for the next activation of this object or to view the profile you have selected. The setting applies to the instance of the object contained in the group specified on the **Instance Information** tab of its **Details** task. More than one system defined or user-defined custom group can contain a unique instance of the same object; this situation allows assigning different activation profiles to different instances of the same system or image. You can set different activation profiles for a single system or image by invoking its **Details** task from the different groups containing the object and selecting **Change Options...**.

Currently assigned profile
Specifies the profile name that has been assigned to this object for this group.

Profile to be assigned

Specifies the profile name you supplied or selected from the list provided.

Profile Name
Displays the name of the profile.

Type
Identifies the general contents and use of the profile.

Image
Indicates the profile can be used to activate an image of a CPC.

Load
Indicates the profile can be used to activate a Central Processor Complex (CPC) or an image and load a control program or operating system.

Reset
Indicates the profile can be used to activate a CPC.

Profile Description
Displays additional information about the profile, such as its specific contents or use.

Note: A description is an optional profile parameter; some profiles may not have one. The person who customizes the profile provides or omits its description.

OK
To assign the selected profile to be used during system activation, click **OK**.

View
To view the contents of the selected activation profile, click **View**.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Adapter Details

Accessing the Adapter Details task

Use this task for information about the selected adapter that is enabled. This window displays the current instance information and acceptable status settings for a selected adapter.

You can access this task from the main console page by selecting the System Management node, by selecting a specific adapter, or by selecting this task in the Tasks index. You can use either the default

SYSPROG user ID or any user IDs that a system administrator has authorized to this task through customization controls in the **User Management** task.

To display and view the details for the selected adapter, complete the following steps.

1. Select the PCHID you want to view adapter details.
2. Open the **Adapter Details** task. The Adapter Details window is displayed.
3. Review the settings under Acceptable Status. Optionally, use its check boxes and click **Apply** to change the acceptable status settings.

Adapter details

This window displays current information and acceptable status settings for the selected adapter.

- **General** includes general information about the adapter's operating conditions and characteristics.
- **Status** includes the current status, state, and acceptable status. Acceptable status settings determine which of the adapter statuses are acceptable and which statuses are unacceptable.

  Review the settings under **Acceptable status**. Optionally, use its check boxes and click **Apply** to change the acceptable status settings.
- **Partitions** includes information on the associated CHPIDs, Cryptos, or FIDs defined for the selected adapter for all partitions.

General

Use the General details section to view information for the selected adapter:

Name:
Indicates the name of the target adapter, which can be 1 - 64 characters in length. Supported characters are alphanumeric, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters. An adapter name must uniquely identify the adapter from all other adapters defined on the same system.

System:
Displays the name for the system.

Location:
Displays the location number of the cage and card slot in which the adapter's hardware is installed. Displays the position number on the card in the slot of the adapter's jack.

Type:
Displays the adapter type of the target adapter.

Size (GiB)
Displays the NVMe adapter size in Gibibyte.

Vendor ID
Displays the manufacturer of the installed SSD for the target NVMe adapter.

Subsystem vendor ID
indicates the manufacturer of the installed SSD for the target NVMe adapter.

Serial number
Displays the serial number of the installed SSD for the target NVMe adapter.

Model number
Displays the model number of the installed SSD for the target NVMe adapter.

Swapped with:
Displays the name of the adapter that it is swapped with. If the adapter is not swapped, this field displays none (displays for FICON Express).

Operation mode:
Displays mode of operation for the targeted adapter (displays for Internal Couplings, FICON Express, OSA-Express, Coupling Express LR Channel, Integrated Coupling Adapter SR, HiperSockets).

Network IDs:
Identifies the physical layer 2 LAN fabric or physical broadcast domain. You can use this value to logically associate the system features, adapters, and ports to be physically connected to your network (displays for Internal Shared Memory, OSA-Express, RoCE adapters).

Physical adapter ID:
Indicates the physical adapter ID for the selected adapter (displays for Coupling Express LR, Integrated Coupling Adapter SR).

Port:
Displays the adapter port number (displays for Coupling Express LR, Integrated Coupling Adapter SR).

Status

Status settings determine which of the adapter statuses are acceptable and which statuses are unacceptable:

Status

Indicates the status of the target adapter. This field can indicate Operating or Not Operating. This field is updated dynamically, so that it always reflects the current status of the target adapter.

State

Indicates the state of the adapter. This field can indicate Online or Offline. This field is updated dynamically, so that it always reflects the current state of the target adapter.

Acceptable status

This term indicates the summarized status of the adapters.

- Acceptable statuses, indicated by check marks in their check boxes, are not reported as exceptions.
- Unacceptable statuses, indicated by empty check boxes, are reported as exceptions.
- Check boxes are disabled, if the user does not have **Adapter Details** task permission.

Settings determine which of the adapter statuses are acceptable and which statuses are unacceptable. Setting the adapter's acceptable status settings allows you to control which statuses are reported as exceptions. The following adapter status values can be summarized as acceptable:

Operating
The adapter is operating.

Suspended
The adapter is suspended. The adapter is not operating.

No Power
The power is off for the hardware that supports the adapter. The adapter is not operating.

Service
The adapter is in single channel service (SCS) mode and is not in the active I/O configuration. The adapter is not operating.

Not Defined
The adapter is not defined in the active IOCDS. The adapter is not operating.

Definition error
The adapter specified in the active input/output configuration data set (IOCDS) does not match the characteristics of the installed adapter, or the adapter type is incompatible with the current storage allocation, or the level of the installed adapter hardware does not support the definition in the IOCD. The adapter is not operating.

Wrap block
A wrap block is installed on the adapter's interface.

Note: Wrap blocks are used during special diagnostic tests performed on the adapter. Wrap blocks must be removed prior to system initialization to allow the adapter to initialize completely. The adapter is not operating.

Check stopped
The adapter is unavailable due to a permanent machine error affecting the adapter hardware. The adapter is not operating.

Permanent error
The adapter is unavailable due to a permanent outboard error. The adapter is not operating.

Loss of signal
The adapter detected a link-signal error. The level of the signal on the link is below the value specified for reliable communication.

Loss of synchronization
The adapter detected a link-signal error. The bit synchronization with the signal was lost. The adapter is not operating

Not operational link
The adapter detected a link failure due to a not-operational sequence. The channel path is not operating.

Sequence time-out
The channel path detected a link failure due to a sequence time out. The adapter is not operating.

Sequence not permitted
The adapter detected a link failure due to an illegal sequence for a link. The adapter is not operating.

Terminal condition
The adapter is not available due to an interface-hung condition. This can occur after an interface or adapter error if the control unit or device fails to disconnect from the interface when requested by the adapter. The adapter is not operating

Offline signal received
The adapter detected an offline sequence, indicating that the sender is in offline mode and subsequent link-signal errors detected by the adapter are not to be reported. For an ES conversion adapter, this condition can occur only when the adapter is wrongly attached to another adapter, switch, or control unit instead of an ESCON Converter. The adapter is not operating.

Initializing
The firmware is being loaded into the adapter card and then the adapter card is starting.

Degraded
A degraded status indicates that, although the adapter is still operating, some conditions are causing a degraded status.

Test mode
The adapter is in test mode. The adapter is not operating

Bit error threshold exceeded
The number of bit errors the adapter detected while receiving or sending data is more than the threshold set for its bit error counter. The adapter is not operating

IFCC threshold exceeded
The number of interface control checks (IFCCs) the adapter detected is more than the threshold set for its IFCC counter. IFCCs may continue to occur, but their error logs will not be created and sent to the Support Element.

Stopped
The channel path is not operating.

I/O suppressed
The adapter has input/output (I/O) suppression active. I/O suppression prevents the adapter subsystem from selecting any device and fetching the first adapter command word (CCW) of a adapter program. The adapter is not operating.

Fabric login sequence failure
This condition means that the adapter detected a failure during that fabric login procedure

Port login sequence failure
This condition means that the adapter detected a failure during the registration procedure. In order for a FICON® adapter to communicate with devices on a control unit, it must perform a Port Login with that control unit.

State change registration failure
This condition means that the adapter detected a failure during the registration procedure. A FICON adapter is required to register with the switch to receive state change notification

Invalid attachment failure
Occurs when the adapter determines that it is connected to a switch, but the IOCDS specifies that is should be directly connected to a control unit or the contrary.

Note: The settings of each adapter determine whether the adapter status values are summarized as not operating or acceptable.

Apply acceptable status settings to all adapters
Select this to apply all the selected status settings.

Partitions

The Partitions section displays the Channel Path IDs (CHPIDs), Crypto, or FID depending on the type of adapter defined for the selected adapter for all partitions:

Partition Name
Displays the name of the partition for the targeted adapter.

Partition Status
Indicates the status of the partition for the targeted adapter.

CSS.CHPID/Crypto/FID
Displays all the CSS.CHPIDs, Cryptos, or FIDs associated with that physical channel identifier (PCHID). A CSS identifies which channel subsystems the CHPID belongs to.

The navigation pane also can include the following links to related tasks depending on the selected adapter type:

Advanced facilities
Opens the **Advanced facilities** task for the selected adapter.

Channel problem determination
Opens the **Channel problem determination** task for the selected adapter.

View adapter security
Opens the **View adapter security** window for some selected adapters.

Additional functions on this window include:

Cancel
To exit the window, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Apply
To apply changes you made to the adapter's acceptable status settings, click **Apply**. The **Apply** button is not displayed in view-only mode.

Help
To display help for the current window, click **Help**.

Advanced Facilities

Accessing the Advanced Facilities task

You can use the console workplace to open a facility for monitoring, operating, and customizing a selected channel type. To work with the selected channel type:

Note: Depending on your user task role, you may only be able to view this task.

1. Open the **Advanced Facilities** task.
2. The Advanced Facilities window displays a list of actions you can take depending on the channel type selected. The list may include:
   - **View code level**
   - **Card Trace/Log/Dump Facilities**
   - **Card specific advanced facilities**
   - **Reset to defaults...**
3. Select the action that you want to start, then click **OK**.
4. The next window that displays depends on the action selected:
   - For the Advanced Facilities window, select one of the tasks, then click **OK**.
   - For the View Code Level window, view the code level for the card, then click **OK**.
   - For the Card Trace/Log/Dump Facilities window, select one of the tasks, then click **OK**.
   - For the Reset to Default Configuration window, click **Yes** to reset to the default configuration.

Advanced Facilities

Use this window to select a function to monitor, operate, or customize a selected channel type for the system. The list of actions you can take from the list depends on the channel type selected. The list may include:

- Force error recovery log
- Card display or alter memory...
- View code level
- Card trace/log/dump facilities
- “Card Specific Advanced Facilities” on page 311
- Look up generic access...
- Reset to defaults...

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Force log

Use this window to select a force log function for the selected Coupling Express (CE) LR or Integrated Coupling Adapter (ICA) SR channel type in the system.

Channel ID:
Displays a four-digit physical channel identifier (PCHID) of the selected Coupling Express (CE) LR or Integrated Coupling Adapter (ICA) SR defined channel type.

Channel type:
Identifies specific channel type

Card description:
Displays the card description for the channel type.

Select a force log function for the selected Coupling Express (CE) LR or Integrated Coupling Adapter (ICA) SR channel type:

- Force adapter error recover log

- Force port error recover log
- Force channel error recover log
- Force adapter log
- Force port log
- Force channel log

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Card Specific Advanced Facilities

Use this window to select a card specific function for a selected channel type for the system. The list of card specific facilities actions you can take from the list depends on the channel type selected. The list may include:

- Query port status...
- View port parameters...
- Display or alter MAC address...
- Enable or disable ports...
- Run port diagnostics
- Set card mode...
- Display client connections...
- Display active sessions configuration...
- Display active server configuration...
- Panel configuration options...
- Manual configuration options...
- Activate configuration
- Display activate configuration errors...
- Debug utilities...
- Manage security certificates...

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Query port status

Displays the local area network (LAN) port record of each LAN port on the selected Open Systems Adapter (OSA)-Express® channel.

A LAN port record:

- Displays the port identifier
- Indicates whether the port is enabled or disabled
- Indicates whether the port is in Support Element control mode
- Indicates the source of the command that disabled the port if the port becomes disabled while it is not in Support Element control mode.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected OSA-Express channel can be connected to through cable connections to its port or ports.

Query port table

First line list column:

Port ID
Displays the number that uniquely identifies the port on the OSA-Express card.

Type
Identifies the type of LAN supported by the port.

Port state
Indicates the current state of the port.

Disabled
Indicates if the port was disabled by the Support Element.

External disabled
Indicates if the port was disabled by an external LAN request.

Host program disabled
Indicates if the port was disabled by a host support program.

Second line list column:

Port ID
Displays the number that uniquely identifies the port on the OSA-Express card.

Support Element Control Mode
Indicates if the port accepts commands only from its Support Element.

Port Configuration Change
Indicates if the port has changed configuration.

Port Failure
Indicates if a licensed internal code problem has occurred which stops the port from being enabled.

Link Threshold Exceeded
Indicates if the port has been disabled because the number of link failures has exceeded the threshold.

Link Monitor
Describes why the port is in Link Monitor State. This is a bit field. The bits are numbered from left (bit 0) to right (bit 15).

- Bit 0: *loss of signal* - most likely cause is an improperly installed or broken cable. Please check your connection or cable.
- Bit 1: *not used*.
- Bit 2: *registration failure* - registration was rejected by ATM switch or the switch is not operational. This is most likely the result of the configuration not matching the configuration of the LES. Fix the configuration and make sure that the required switch is operational.
- Bit 3: *loss of SAAL connection* - this is set when there is a problem with the communication to the switch. Have your network person check the switch connection.

- Bit 4-15: *Reserved*

Definition Error Code
Describes why the port is in Definition Error State.

- "00" - Unspecified Error
- "01" - Invalid Type
- "02" - Invalid Parameter

Additional functions on this window include:

OK
To close the window when you finish reviewing the LAN port records, click **OK**.

Help
To display help for the current window, click **Help**.

Query port status

Displays the local area network (LAN) port record of each LAN port on the selected Open Systems Adapter (OSA)-Express channel.

A LAN port record:

- Displays the port identifier
- Indicates whether the port is enabled or disabled
- Indicates whether the port is in Support Element control mode
- Indicates the source of the command that disabled the port if the port becomes disabled while it is not in Support Element control mode.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected OSA-Express channel can be connected to through cable connections to its port or ports.

Query port status table

Port Identifier
Displays the number that uniquely identifies the port on the OSA-Express card.

Type
Identifies the type of LAN supported by the port.

Port State
Indicates the current state of the port.

Disable
Indicates if the port was disabled by the Support Element.

Support Element Control Mode
Indicates if the port accepts commands only from its Support Element.

Port Block
Indicates the port was disabled by a LAN request.

External Disabled
Indicates if the port was disabled by an external LAN request.

Internal Port Failure
Indicates if a licensed internal code problem has occurred which stops the port from being enabled.

Additional functions on this window include:

OK
To close the window when you finish reviewing the LAN port records, click **OK**.

Help
To display help for the current window, click **Help**.

View port parameters

The view port parameters window displays various information about the selected port on the channel. This information (which varies based on channel hardware type and specified CHPID type) can contain state, current connection speed/mode, configured speed/mode, counter for various data items processed, as well as counters for various errors detected.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected zHyperLink or RoCE Express2 channel.

Port
Identify the physical port of the selected zHyperLink or RoCE Express2 channel.

Additional functions on this window include:

Close
To close the current window, click **Close**.

Export to USB Device
To export the selected channel port parameter data to a USB Device, click **Export to USB Device**.

Export to FTP Server
To export the selected channel port parameter data to an FTP Server, click **Export to FTP Server**.

Help
To display help for the current window, click **Help**.

View port parameters

The view port parameters window displays current power optic (receiver and transmit) measurement information about the selected FICON port on the adapter.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected FICON adapter.

Additional functions on this window include:

Close
To close the current window, click **Close**.

Help
To display help for the current window, click **Help**.

Display MAC address

Displays the medium access control (MAC) addresses of the ports on the selected RoCE Express channel.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected RoCE channel.

LAN port type
Identifies the type of network the selected RoCE channel can be connected to through cable connections to its port or ports.

LAN port *n* MAC address
Displays the current medium access control (MAC) address of port number *n*. Each field in the group displays the hexadecimal value of one byte in the 6-byte (48-bit) MAC address of the port. The leftmost field displays byte 0; the rightmost field displays byte 5.

Additional functions on this window include:

Retrieve Universal MAC
To display the universally administered medium access control (MAC) address of each port, click **Retrieve Universal MAC**.

Note: This only displays each port's universal MAC address in its **MAC address LAN port *n*** field.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Display or alter MAC address

Displays the medium access control (MAC) addresses of the ports on the selected Open Systems Adapter (OSA)-Express channel.

You can also use the window to change one or more MAC addresses.

Note: This window might only allow view only for some user task roles.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

MAC address LAN port *n*
Initially displays the current medium access control (MAC) address of port number *n*. Each field in the group displays the hexadecimal value of one byte in the 6-byte (48-bit) MAC address of the port. The leftmost field displays byte 0; the rightmost field displays byte 5.

Use the fields to change the MAC address of the port.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Retrieve Universal MAC
To display the universally administered medium access control (MAC) address of each port, click **Retrieve Universal MAC**.

Note: This only displays each port's universal MAC address in its **MAC address LAN port *n*** field.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Enable or disable port (Coupling Express LR and Integrated Coupling Adapter SR)

Use this window to enable or disable the local area network (LAN) ports for the selected Coupling Express (CE) LR or Integrated Coupling Adapter (ICA) SR channel type and to set the Support Element control mode of the port.

Channel Path
Displays a four-digit physical channel identifier (PCHID) of the selected channel.

Channel type
Identifies the type of network the selected Coupling Express (CE) LR or Integrated Coupling Adapter (ICA) SR channel type can be connected to through cable connections to its port or ports.

Identify the desired physical port state:

Enable physical port
Enable a port to allow it to communicate with other devices attached to the LAN. An enabled port can receive information from other devices attached to the LAN, and can send information to them.

Disable physical port
Disable a port to prevent it from communicating with other devices attached to the LAN.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Enable or disable port

Use this window to enable or disable the local area network (LAN) ports for the selected Open Systems Adapter (OSA)-Express channel and to set the Support Element control mode of the port.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Attention: Make sure the port is not being used by other partitions before it is disabled.

Port number
Identify the port of the selected Open Systems Adapter (OSA)-Express channel.

Port status commend

Enable port
Enable a port to allow it to communicate with other devices attached to the LAN. An enabled port can receive information from other devices attached to the LAN, and can send information to them.

Disable port
Disable a port to prevent it from communicating with other devices attached to the LAN.

Support Element control code command

Set control on
Set the Support Element control mode of a port on.

Set control off
Set the Support Element control mode of a port off.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Run adapter diagnostics

Use this window to test the hardware of local area network (LAN) ports on the selected RoCE channel type for the system.

Attention: A diagnostic test cannot be stopped once it has started.

When testing is complete, a message will display to indicate whether the test completed with errors or without errors. In either case, the tested port will be displayed to show the results of the testing.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected RoCE channel.

Type of Diagnostic Test:
Click **Self test** to request basic card diagnostics performed to validate that the card hardware is acceptable.

Click **Functional test** to request running an internal or external simulated workload (for example: RoCE Ethernet traffic) to validate that the card can perform its assigned task.

Loopback:

Click **Internal** to request a functional test executed internally on the card.

Click **External** to request a functional test executed with a wrap cable to test port hardware that supports the external connection of the specified port to a local area network (LAN). The port must be disabled and the wrap plug must be installed on the card.

Additional functions on this window include:

OK

To continue with the operation, click **OK**.

Cancel

To close the window and exit the task, click **Cancel.**

Help

To display help for the current window, click **Help**.

Run port diagnostics

Use this window to view the sense data set during diagnostic testing of an Open Systems Adapter (OSA)-Express port.

The sense data indicates the results of running diagnostics.

Channel ID

Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type

Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Sense data

LAN port status word 0 displays the hexadecimal values of sense data bytes 0, 1, 2, and 3.

LAN port status word 1 displays the hexadecimal value of sense data bytes 4, 5, 6, and 7.

LAN port status word 2 displays the hexadecimal values of sense data bytes 8, 9, 10, and 11.

LAN port status word 3 displays the hexadecimal values of sense data bytes 12, 13, 14, and 15.

LAN port status word 4 displays the hexadecimal values of sense data bytes 16, 17, 18, and 19.

LAN port status word 5 displays the hexadecimal values of sense data bytes 20, 21, 22, and 23.

LAN port status word 6 displays the hexadecimal values of sense data bytes 24, 25, 26, and 27.

LAN port status word 7 displays the hexadecimal values of sense data bytes 28, 29, 30, and 31.

Additional functions on this window include:

OK

To continue with the operation, click **OK**.

Cancel

To close the window and exit the task, click **Cancel.**

Help

To display help for the current window, click **Help**.

Set card mode or speed

Use this window to set transmission settings for local area network (LAN) ports on the selected Open Systems Adapter (OSA)-Express channel. You can set the transmission mode of local area network (LAN) ports.

Channel ID

Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Physical port identifier
Identify the physical port of the selected Open Systems Adapter (OSA)-Express channel.

Mode

Select the transmission mode you want to set for the port when the selected Open Systems Adapter (OSA)-Express channel can be connected to a local area network (LAN).

Full duplex
Enable sending and receiving data transmissions at the same time.

Half duplex
Enable sending and receiving data transmissions, but not at the same time.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Set card mode or speed

Use this window to set transmission settings for local area network (LAN) ports on the selected Open Systems Adapter (OSA)-Express channel. You can set the transmission speed and mode of local area network (LAN) ports.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Physical port identifier
Identify the physical port of the selected Open Systems Adapter (OSA)-Express channel.

Mode/speed

Select the transmission speed and mode you want to set for the port when the selected Open Systems Adapter (OSA)-Express channel can be connected to a local area network (LAN).

Auto Negotiate
Set the port at the current network speed.

Mode/Speed
Set the transmission speed and mode you want for the port.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

Set card mode or speed

Use this window to set transmission settings for local area network (LAN) ports on the selected Open Systems Adapter (OSA)-Express channel. You can set the transmission speed and mode of local area network (LAN) ports.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Physical Port
Identify the physical port of the selected Open Systems Adapter (OSA)-Express channel.

Mode/speed

Select the transmission speed and mode you want to set for the port when the selected Open Systems Adapter (OSA)-Express channel can be connected to a local area network (LAN).

Auto Sense
Set the port at the current network speed.

Speed/Mode
Set the transmission speed and mode you want for the port.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel.**

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Display client connections

Use this window to display Network Interface Card information for the selected Open Systems Adapter (OSA)-Express channel.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Client connections table

Session Index
Displays the session numbers for the selected OSA-Express channel. A valid range for the session numbers is 0 to 120.

Status
Displays one of the following client session connections for the selected OSA-Express channel:

- **Ready** - Indicates the session has been configured and the client can be connected.
- **Active** - Indicates the session has been configured and the client is connected.
- **Not configured** - Indicates the session has not yet been configured.
- **Definition error** - Indicates the session is not a valid session and the client cannot connect.
- **Connected** - Indicates the session has been configured and the client is connected to it.

- **DHD Pending** - Indicates the client has been disconnected. However, since DHD was enabled, OSA-ICC has not notified the host operating system.

MAC
Displays the media address control (MAC) address of the client that is being connected. A MAC address identifies a port as a destination and source of information it receives and transmits, respectively, on the local area network (LAN).

Client IP
Indicates the client's IP address.

Port
Indicates the number that identifies the port for the client connection.

Socket Number
Displays the TCP socket number that uniquely defines the connection.

LT Index
Displays the index in the LT table. A valid range for the LT index is 0 to 119.

Connect Rule
Indicates one of the following connect rules:

- IP only
- LU only
- IP and LU
- Unknown

Disable Logo
Displays the OSA-ICC logo that appears when the session is first connected.

Additional functions on this window include:

OK
To close the current window, click **OK**.

Help
To display help for the current window, click **Help**.

Display client connections

Use this window to display Network Interface Card information for the selected Open Systems Adapter (OSA)-Express channel.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Client connections table

Session Index
Displays the session numbers for the selected OSA-Express channel. A valid range for the session numbers is 0 to 120

Status
Displays one of the following client session connections for the selected OSA-Express channel:

- **Ready** - Indicates the session has been configured and the client can be connected
- **Active** - Indicates the session has been configured and the client is connected
- **Not configured** - Indicates the session has not yet been configured
- **Definition error** - Indicates the session is not a valid session and the client cannot connect
- **Connected** - Indicates the session has been configured and the client is connected to it

- **DHD Pending** - Indicates the client has been disconnected. However, since DHD was enabled, OSA-ICC has not notified the host operating system.

Physical Port
Displays the physical port for the selected channel

MAC
Displays the media address control (MAC) address of the client that is being connected. A MAC address identifies a port as a destination and source of information it receives and transmits, respectively, on the local area network (LAN)

Client IP
Indicates the client's IP address

TCP Port
Indicates the number that identifies the port for the TCP connection

Socket Number
Displays the TCP socket number that uniquely defines the connection

LT Index
Displays the index in the LT table. A valid range for the LT index is 0 to 119

Connect Rule
Indicates one of the following connect rules:

- IP only
- LU only
- IP and LU
- Unknown

Disable Logo
Displays the OSA-ICC logo that appears when the session is first connected.

Additional functions on this window include:

OK
To close the current window, click **OK**.

Help
To display help for the current window, click **Help**.

Panel configuration options

Use this window to determine if you can select a configuration option for the selected Open Systems Adapter (OSA)-Express channel to validate the session configuration or view the validate error.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected OSA-Express channel can be connected to through cable connections to its port or ports.

Configuration file options

Edit OAT entries
To open a window to configure OSA Address Table (OAT) entries for the selected OSA defined OSE channel type.

Edit SNA timers
To open a window to configure SNA timer values for the selected OSA defined OSE channel type.

Validate panel values
To open a window to validate panel values for a session configuration for the selected Open Systems Adapter (OSA)-Express channel.

Display validate panel errors
To open a window to display validate panel errors, if any exist.

Note: After the values have been validated, select the Activate configuration option on the Advanced Facilities window to active them or your current changes are lost.

Additional functions on this window include:

OK
To apply the selected options, click **OK**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Edit SNA timers

Use this window select or enter SNA timer values to configure the OSA for the selected OSE defined channel type.

Port Number
Indicate the port number the SNA timers are associated with the selected OSE defined channel type.

Inactivity Timer/Ti (ms)
Use the drop down box to select or type the inactivity timer to be initialized for the selected OSE defined channel type. If the Ti timer is enabled, you can set its timeout value in increments of 0.12 seconds from 0.24 to 90.00 second. An enabled inactivity timer (ti) periodically tests the viability of the network media. The timer setting applies to all the clients on the target LAN, not to individual clients. The timer interval indicates how quickly a failure of the network media can be detected when the connection is quiescent.

Response timer/T1 (ms)
Use the drop down box to select or type the response timer for the selected OSE defined channel type. The T1 timer clocks link events that require responses from clients on the network. T1 can be set to a timeout value from 0.20 up to 51.00 seconds in increments of 0.20 seconds. Set the T1 timer to a value not less than the average round-trip transit time from the OSA to the clients and back.

Acknowledgment timer/T2 (ms)
Use the drop down box to select or type the acknowledgment timer for the selected OSE defined channel type. An OSA starts the T2 timer when it receives an I-format LPDU and stops when it sends an acknowledgment. An acknowledgment is sent either when an outgoing I frame is sent or when N3 number of I-format link protocol data units (LPDUs) has been received. Set a value from 0.08 seconds up to 20.40 seconds in increments of 0.08 seconds.

Maximum Frames Before Transmit Window/N3
Use the drop down box to select or type the maximum frames before transmit window for the selected OSE defined channel type. When determining the maximum I-frames that can be sent before an acknowledgment is sent (N3 count) and the maximum number of outstanding I-format link protocol data units (LPDUs) (TW count), consider the N3 and TW counts that are set at the clients as well.

Maximum Transmit Window/TW
Use the drop down box to select or type the maximum transmit window for the selected OSE defined channel type. The TW count allows the sender to transmit before that sender is forced to halt and wait for an acknowledgment. The TW count can be set as an integer from 1-16.

Additional functions on this window include:

OK
To save the new values, click **OK**.

Cancel
To close the window without saving the current selected changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

Edit/display sessions configuration

Use this window to display or allow you to select a configuration edit session for the selected Open Systems Adapter (OSA)-Express channel. The window displays information that can be configured for the selected OSA-Express channel edit session configuration.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Edit/display sessions configuration table

Session index
Displays the session index number for the selected OSA-Express channel.

State
Displays one of the following sessions configuration states:

- **Available** - Indicates the session has been configured and the client can be connected.
- **Definition error** - Indicates the session is not a valid session and the client cannot connect.
- **Not configured** - Indicates the session has not yet been configured.

CSS
Displays the channel subsystem (CSS). A valid range for the CSS is 0 to 3.

MIFID
Displays the logical partition ID. A valid range for the Image ID is 1 to F.

Device Number
Displays a unique number that is assigned for each device that was defined in the IOCDS.

LU Name (3270 OSC OSA channels only)
Indicates what active session you are connecting to. The LU name defines a group pool of devices.

Client IP
Indicate the IP address that a client will use to connect to the session. The client IP address can remain 0.0.0.0 or empty in order to allow any client to connect to a specific session. If a nonzero IP is specified, any client with a nonmatching IP will be rejected.

IP Filter
Displays the IP Filter address that is used for routing to specific subnets.

Session Type (3270 OSC OSA channels only)
Displays one of the following active session types for the selected OSA-Express channel:

- **TN3270**
- **Operator console**
- **Printer**

Defer host disconnect (DHD) (3270 OSC OSA channels only)
Displays the defer host disconnect (DHD) time for the active session configuration to wait until the session instructs the host it has disconnected. The defer host disconnect can be:

- **Disable**
- **Enable with defaulted deferment of 60 seconds**
- **Enable with no timeout for deferment**
- **Enable with user specified defaulted deferment**

Response mode (RSP) (3270 OSC OSA channels only)
Displays the response mode (RSP) for the active session configuration. The response mode is either:

- **Enable** - Allows the host to wait for the client to send an acknowledgment on the Telnet level for every packet that is transmitted.
- **Disable** - Prevents the client from sending an acknowledgment.

Read Timeout (RTO) (3270 OSC OSA channels only)
Displays the read timeout (RT0) for the active session configuration to wait (in seconds) for a response from the client before performing a client disconnect. The read timeout can be:

- **Disable**
- **Low (1 second)**
- **Medium (10 seconds)**
- **High (60 seconds)**
- **User specified timeout**

Additional functions on this window include:

OK
To close the window when you finish reviewing the sessions, click **OK.**

Save
To save edit session data, click **Save**.

Change
To change edit session data, select a line and click **Change**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window.

Edit sessions configuration

Use this window to select a configuration session for the selected Open Systems Adapter (OSA)-Express channel. The window displays information that can be configured for the selected OSA-Express channel session configuration.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Edit sessions configuration table

Session Index
Display the session index number for the selected OSA-Express channel.

State
Display one of the following sessions configuration states:

- **Available** - Indicates the session has been configured and the client can be connected.
- **Definition error** - Indicates the session is not a valid session and the client cannot connect.
- **Not configured** - Indicates the session has not yet been configured.

CSS Value
Display the channel subsystem (CSS). A valid range for the CSS is 0 to 3.

MIFID
Display the logical partition ID. A valid range for the Image ID is 1 to F.

Device Number
Display a unique number that is assigned for each device that was defined in the IOCDS.

LU Name
Indicate what active session you are connecting to. The LU name defines a group pool of devices.

Client's IP
Indicate the IP address that a client will use to connect to the session. The client's IP address can remain 0.0.0.0 or empty in order to allow any client to connect to a specific session. If a nonzero IP is specified, any client with a nonmatching IP will be rejected.

IP Filter
Display the IP Filter address that is used for routing to specific subnets.

Session Type
Display one of the following active session types for the selected OSA-Express channel:

- **TN3270**
- **Operator console**
- **Printer**

Defer host disconnect (DHD)
Display the defer host disconnect (DHD) time for the active session configuration to wait until the session instructs the host it has disconnected. The defer host disconnect can be:

- **Disable**
- **Enable with defaulted deferment of 60 seconds**
- **Enable with no timeout for deferment**
- **Enable with user specified defaulted deferment**

Response mode (RSP)
Display the response mode (RSP) for the active session configuration. The response mode is either:

- **Enable** - Allows the host to wait for the client to send an acknowledgment on the Telnet level for every packet that is transmitted.
- **Disable** - Prevents the client from sending an acknowledgment.

Read Timeout (RTO)
Display the read timeout (RT0) for the active session configuration to wait (in seconds) for a response from the client before performing a client disconnect. The read timeout can be:

- **Disable**
- **Low (1 second)**
- **Medium (10 seconds)**
- **High (60 seconds)**
- **User specified timeout**

Additional functions on this window include:

Save
To save session data, click **Save**.

Change
To change session data, select a line and click **Change**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Edit session configuration

Use this window to change a configuration session for the selected Open Systems Adapter (OSA)-Express channel.

Channel ID
Display a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identify the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Session Index
Display the session number for the selected OSA-Express channel.

Session State
Display one of the following sessions configuration states:

- **Available** - Indicates the session has been configured and the client can be connected.
- **Active** - Indicates the session has been configured and the client is connected.
- **Connected** - Indicates the session has been configured and the client is connected to it.
- **Definition error** - Indicates the session is not a valid session and the client cannot connect.
- **Not configured** - Indicates the session has not yet been configured.

CSS Value
Use the drop down box to select or type the channel subsystem (CSS) value for the session configuration of the selected Open System Adapter (OSA)-Express channel. A valid range for the CSS is 0 to 3.

MIFID
Use the drop down box to select or type the logical partition ID for the session configuration of the selected Open Systems Adapter (OSA)-Express channel.

Device Number
Use the drop down box to select or type the unique number for each device for the session configuration of the selected Open System Adapter (OSA)-Express channel.

LU Name
Enter the session you are connecting to for the selected Open Systems Adapter (OSA)-Express channel. The LU name defines a group pool of devices.

Client's IP address
Enter the client's IP address for the selected OSC channel. This entry field is optional.

IP Filter
Enter the IP filter address that is used for routing to specific subnets.

Session Type
Select one of the following choices to indicate the session type for the selected Open Systems Adapter (OSA)-Express channel.

- **TN3270**
- **Operator console**
- **Printer**

Defer host disconnect
Select a one of the following to indicate the type of defer host disconnect (DHD) you want the session configuration to wait before instructing the host to disconnect.

- **Disable**
- **Enable with defaulted deferment of 60 seconds**
- **Enable with no timeout for deferment**
- **Enable with user specified defaulted deferment**

Defer host disconnect time value (seconds)
Enter your own defer host disconnect (DHD) time value in seconds that you want to specify for the session to wait before instructing the host to disconnect.

Response mode
Select a response (RSP) mode choice for the host to wait for the client to respond to the last packet of data. The response mode is either:

- **Enable** - Allows the host to wait for the client to send an acknowledgment on the Telnet level for every packet that is transmitted.
- **Disable** - Prevents the client from sending an acknowledgement.

Read Timeout
Select a choice to indicate the read timeout (RTO) for a response (in seconds) from the client before instruction the host to perform a disconnect. The read timeout can be:

- **Disable**
- **Low (1 second)**
- **Medium (10 seconds)**
- **High (60 seconds)**
- **User specified timeout**

Read timeout value
Enter your own read timeout (RTO) response (in seconds) value you want to specify for the session to wait before instructing the host to disconnect.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Delete Session
To delete the currently selected sessions configuration, click **Delete Session**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Display/Edit server configuration

Use this window to enter server configuration information for selected channel.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Physical Port 0/1

You can edit the server configuration information for the selected channel. To define a physical port, valid parameter values must be entered as displayed on the ranges adjacent to the parameter field. If a physical port is not defined, the IP address, Gateway, and TCP Port must all be set to 0 and the Prefix must be set to 1.

Note: By default all physical port parameters are set to 0. If the default value of 0 is not present in the IP address, Gateway, and TCP Port and 1 is not present in the in the Prefix physical port fields, that physical port is considered defined.

Server name
Enter the server name that the client is connected to for the selected Open Systems Adapter (OSA)-Express channel.

Enable IPv4
Check this box to enable IPv4

Host IPv4 address
Enter the host IP4v address for the active server configuration

Prefix
Enter the prefix of the IPv4 address for the active server configuration

IPv4 TCP port
Enter the IPv4 TCP port identifier for the active server configuration

IPv4 secure TCP port
Enter the IPv4 secure TCP port identifier for the active server configuration

Enable IPv6
Check this box to enable IPv6

Address type
Use this pull down to select the address for this IPv6 address

Host IPv6 address
Enter the host IPv6 address for the active server configuration

Prefix
Enter the prefix of the IPV6 address

IPv6 TCP port
Enter the IPv6 TCP port identifier for the active server configuration

IPv6 secure TCP port
Enter the IPv6 secure TCP port identifier for the active server configuration.

MTU size
Enter the maximum transfer (MTU) size to be transferred in one frame. A valid range is from 256 to 1492.

TLS version
Use this pull down to select the TLS version

- Select TLS 1.0 protocol version means ICC 3270 server allows secured client connections for protocols TLS 1.0, TLS 1.1, and TLS 1.2
- Select TLS 1.1 protocol version means ICC 3270 server allows secured client connections for protocols TLS 1.1 and TLS 1.2
- Select TLS 1.2 protocol version means ICC 3270 server allows secured client connections for protocols TLS 1.2 .

IPv4 default Gateway
Enter the IPv4 default gateway. The IPv4 default gateway is the network that connects the hosts

IPv6 default Gateway
Enter the IPv6 default gateway. The IPv6 default gateway is the network that connects the hosts.

Additional functions on this window include:

OK
To apply the changes displayed in the fields, click **OK**.

Close
To close the window without saving the current selected changes, click **Close**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Display/Edit server configuration

Use this window to enter server configuration information for selected channel.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Physical Port 0/1

You can edit the server configuration information for the selected channel. To define a physical port, valid parameter values must be entered as displayed on the ranges adjacent to the parameter field. If a physical port is not defined, the IP address, Gateway, and TCP Port must all be set to 0.

Note: By default all physical port parameters are set to 0. If the default value of 0 is not present in the IP address, Gateway, Subnet Mask, and TCP Port physical port fields, that physical port is considered defined.

Server name
Enter the server name that the client is connected to for the selected Open Systems Adapter (OSA)-Express channel.

Host IP address
Enter the host IP address for the active server configuration.

TCP port
Enter the TCP port identifier for the active server configuration.

Secure TCP port
Enter the secure TCP port identifier for the active server configuration.

Subnet Mask
Enter the subnet mask. The subnet mask identifies the TCP/IP protocol that is used for routing to specific subnets.

Default Gateway
Enter the default gateway. The default gateway is the network that connects the hosts.

MTU Size(B)
Enter the maximum transfer unit (MTU) size to be transferred in one frame. A valid range is from 256 to 1492.

Frame types

Select a choice to indicate the Ethernet standards that you want the network to follow. Every host in a network must have the same frame type.

DIX
Select the DIX frame type for the session configuration. It is **strongly recommended** that you use DIX as your frame type.

SNAP
Select the SNAP frame type for the session configuration.

Note: The recommended frame type for OSA-ICC is DIX. Changing the frame type to another mode without checking with your Network Administrator could cause a loss of data.

Additional functions on this window include:

OK
To apply the changes displayed in the fields, click **OK**.

Close
To close the window without saving the current selected changes, click **Close**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Manual configuration options

Use this window to select the manual configuration option for the session configuration of the selected Open Systems Adapter (OSA)-Express channel. You can export a session source file to a media source, then edit the file on your workstation with an editor. After you have completed editing your file, import the session source file back on the Support Element using the import source file choice.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Configuration file options

Import source file
Import a session configuration file that was exported to a diskette for editing.

Note: In order to make the imported edited source file the active configuration, you must *Validate source file* and then *Activate configuration*.

Insert the media source containing the source file into your disk drive, then highlight the file you would like to import and click **OK**.

Export source file
Export a session configuration file to a media source to edit with your workstation editor. You can also use this panel to export your configuration file as a backup.

Insert the media source containing the source file into your disk drive, then type the name to be given to the exported configuration file in the field and click **OK**.

Import source file by FTP
Import a session configuration file from a designated FTP site.

Export source file by FTP
Export a session configuration file to a designated FTP site.

Load default source file
To load the default source file.

Edit source file
Edit the session source configuration file.

Validate source file
Validate the session source configuration file to ensure that the file is valid before activating it. **Attention:** In order to make the validated source file the active configuration, you must activate it. Activating a configuration makes any changes you made effective immediately. This could result in active sessions being dropped.

If the source file you are validating is incorrect, the errors and warnings will be commented in the source file. You must fix any errors before activating your configuration. When the validate is successful, you will receive a message stating that your source file is successful, then click **OK**.

Note: After the source file has been validated, select the Activate configuration option on the Advanced Facilities window to active them or your current changes are lost.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Import Source File

Select **Import Source File** to copy a configuration source file from one medium to the Support Element.

The import function copies a source file from the FTP destination to the Support Element hard disk.

Use the **Protocol** field to select a secure network protocol for transferring files to the specified FTP destination. Use the **File path** field to type the file path directory where the files are to be saved or read.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

Additional functions on this window include:

Import
To import data configuration files from a FTP destination, click **Import**.

Cancel
To close the window without saving your changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

Export Source File

Select **Export Source File** to export a configuration source file from the Support Element hard disk to an FTP destination.

The export function copies a source file from the Support Element to an FTP destination.

Use the **Protocol** field to specify a secure network protocol for transferring files to the specified FTP destination. Use the **File path** field to type the file path directory where the files are to be saved or read.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the file path and the file name of the data file that is to be saved.

Additional functions on this window include:

Export
To export configuration data files to an FTP destination, click **Export**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Debug utilities

Use this window to select a debug option for the selected Open Systems Adapter (OSA)-Express channel. This window identifies the channel ID and LAN port type of the selected OSA-Express channel.

Ping utility
Select the ping utility to ping an active session to verify the status of the connection.

Trace route utility
Select the trace route utility to trace the route of a packet of data to a session.

Drop session
Select drop session to enter the session number to drop for the ping utility to identify.

Logo controls
Select the logo controls to enter the operating system session number to enable or disable a three line logo screen.

Query command
Select the query command to enter a command to the OSC channel for information.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Ping utility

Use this to open a window to ping an active session to verify the status of the connection.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Client IP address
Indicate the client's IP address.

Length (in bytes)

Use this entry field to indicate the ping custom length of 8 to 32000 bytes.

Default (256)
Use the length default value. The default length value is 256 bytes.

Custom length
Set your own custom length of 8 to 32000 bytes.

Count

Use this entry field to indicate a custom count for the ping between 1 and 10.

Default (1)
Use the count default value. The default count value is 1.

Custom count
Set a custom count for the ping between 1 and 10.

Timeout (in seconds)

Use this entry field to indicate you own ping custom timeout value.

Default (1)
Use the timeout default value. The default timeout value is 10.

Custom timeout
Set your own custom timeout value between 1 and 30.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Trace route utility

Opens a window to trace the route of a packet of data to a session.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Client IP address
Indicate the client's IP address.

MAX TTL

Use to select the trace route maximum time to live (TTL) for the packet that is being sent.

Default(30)
Use the MAX TTL default value. The default MAX TTL value is 30.

Custom MAX TTL
Set a custom MAX TTL.

Attempts

Use to select the attempts value for the trace route.

Default(3)
Use the attempts default value. The default attempts value is 3.

Custom attempts
Set a custom attempts value of between 1 and 20.

Port

Use to select the trace route port value you want set for the trace route.

Default(4096)
Use the port default value. The default port value is 4096.

Custom port
Set a custom port identifier between 2048 and 60000.

Wait time in seconds

Default(5)
Use the wait time default value. The default wait time value is 5 seconds.

Custom wait time
Set a custom wait time value of between 1 and 255.

Extra debug messages

No
Do not display extra debug messages.

Yes
Display the extra debug messages.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To close the window without performing the action, click **Cancel.**

Help
To display help for the current window, click **Help**.

Drop session

Use the entry field to identify what session index number to drop.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

Session index
Identify what session index number to drop.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To stop the command currently being processed by the selected channel, click **Cancel.**

Help
To display help for the current window, click **Help**.

Logo controls

Use this window to enter the operating system session index for the selected OSA-Express channel when enabling or disabling a three line logo screen for the operating system screen.

Enable Logo
Clear the operating system screen and display a three line logo screen for the operating system session index entered.

Disable Logo
Do not display a three line logo screen for the operating system session index entered.

Additional functions on this window include:

OK
To close the window after making changes, click **OK**.

Cancel
To close the window without saving the current selected changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

Query command

Use this window to enter a query command to request information from the channel. The query command can be up to 50 alpha-numeric ASCII characters.

Note: This command should be used only under the guidance of service support.

Additional functions on this window include:

OK
To continue with the query command operation, click **OK**.

Cancel
To close the window without saving the current selected changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

Manage security certificate

Use this window to manage Secure Socket Layer (SSL) certificates. Select an action and location to manage the security certificates.

Channel ID
Displays a four-digit physical channel identifier (PCHID) of the selected OSA-Express channel.

LAN port type
Identifies the type of network the selected Open Systems Adapter (OSA)-Express channel can be connected to through cable connections to its port or ports.

OSA-ICC certificate scope
Displays the current OSA-ICC certificate scope that is used for this physical channel identifier (PCHID). Click **Change** to select a different certificate scope action for the selected PCHID.

OSA-ICC certificate type
Displays the OSA-ICC certificate type of this physical channel identifier (PCHID)

OSA-ICC certificate expiration
Displays the OSA-ICC certificate expiration of this physical channel identifier (PCHID).

Actions

- Select **Export self-signed certificate** to generate a self-signed certificate and store in the configuration file to export via USB drive or FTP site
- Select **Reload self-signed certificate** to install the self-signed certificate
- Select **Regenerate OSA-ICC key and self-signed certificate** to regenerate the self-signed certificate
- Select **Create certificate signing request** to generate a certificate signing request and store in the configuration file to export via USB drive or FTP site
- Select **Import signed certificate** to import and install a file via USB drive or FTP site
- Select **View certificate** to view the certificate that is currently being used
- Select **Edit certificate** to edit the certificate signing request (CSR) attributes.

Location

- Select **USB drive** to export or import the selected action
- Select **FTP site** to export or import the selected action.

Additional functions on this window include:

Apply
To save the new values, click **Apply**.

Change
To change the OSA-ICC certificate scope, click **Change**.

Close
To close the window without saving the current selected changes, click **Close.**

Help
To display help for the current window, click **Help**.

Edit Certificate

Use this window to provide the necessary information to create a new certificate or to modify the values of the existing certificate.

Common name
Specify the common name for the certificate

Organization
Optionally, specify the name of the corporation, limited partnership, university, or government agency

Organization unit
Optionally, specify the organization name, which differentiates between divisions within an organization (for example, Hardware Development or Human Resources)

Country or region
Optionally, select or specify the two-character ISO format country code for your country (for example, a two-character code of GB for Great Britain or US for the United States).

You can immediately edit the value that currently appears in the input field or you can select an item that appears from the list.

State or province
Optionally, select or specify the state or province name.

You can immediately edit the value that currently appears in the input field or you can select an item that appears from the list

Locality
Optionally, specify the city or locality name

Valid until
Specify the ending date that the certificate can be valid until, beginning from the time the certificate is created or modified

DNS name
Optionally, add DNS names to the list of valid entries for the certificate

IP Address
Optionally, add IPv4 and IPv6 addresses to the list. The IPv4 address must be specified as 4 decimal numbers separated by a period (for example, dd.ddd.ddd.ddd). The IPv6 address can be specified in several different ways with one form being 8 hexadecimal numbers separated by a colon (for example, xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Email address
Optionally, add email addresses to the list.

Additional functions on this window include:

Save
To save the new values, click **Save**.

Next
To proceed to the next window, click **Next**.

Cancel
To close the window without saving the new values, click **Cancel.**

Help
To display help for the current window, click **Help**.

Export Certificate Signing Request

Use this window to select an export method for the certificate signing request.

Export to FTP
To export to an FTP location, select **Export to FTP**

Export to USB
To export to a USB media, select **Export to USB**

Note: This option is not available remotely.

Export to file system
To export to a local file system, select **Export to file system**

Note: This option is only available remotely.

Additional functions on this window include:

Export
To continue with the selected export method, click **Export**.

Back
To go back to the previous window, click **Back**.

Help
To display help for the current window, click **Help**.

Change OSA-ICC Certificate Scope

Select the certificate scope action that will apply for the PCHID:

Use the shared certificate for this PCHID
Select **Use the shared certificate for this PCHID** to use the shared certificate for this physical channel identifier (PCHID)

Use an individual certificate for this PCHID
Select **Use an individual certificate for this PCHID** to use an individual certificate for this physical channel identifier (PCHID).

Additional functions on this window include:

OK
To save the new values, click **OK**.

Change Certificate Scope
To change the certificate scope, click **Change Certificate Scope**.

Cancel
To close the window without saving the current selected changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Import Source File

Select **Import Source File** to copy a configuration source file from one medium to the Support Element.

The import function copies a source file from the FTP destination to the Support Element hard disk.

Use the **Protocol** field to select a secure network protocol for transferring files to the specified FTP destination. Use the **File path** field to type the file path directory where the files are to be saved or read.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

Additional functions on this window include:

Import
To import data configuration files to an FTP destination, click **Import**.

Cancel
To close the window without saving your changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

Export Source File

Select **Export Source File** to export a configuration source file from the Support Element hard disk to an FTP destination.

The export function copies a source file from the Support Element to an FTP destination.

Use the **Protocol** field to specify a secure network protocol for transferring files to the specified FTP destination. Use the **File path** field to type the file path directory where the files are to be saved or read.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the file path and the file name of the data file that is to be saved.

Additional functions on this window include:

Export
To export configuration data files to an FTP destination, click **Export**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Alternate Support Element

Accessing the Alternate Support Element task

Use this task to perform any of the following actions for the selected CPC:

- Mirror data from the primary Support Element to the alternate Support Element
- Switch from the primary Support Element to the alternate Support Element
- Query whether a switch between Support Elements can take place.

One Support Element is used for the primary, the other as the alternate. The primary Support Element is used for all hardware service. The alternate Support Element has a special workplace window with limited tasks available.

Note: The primary support is scheduled for automatic mirroring by default at 10 a.m. with a one-hour window for starting the operation. A record is added to the Support Element's event log to indicate the outcome of the operation.

Accessing the switching to the primary element and the alternate Support Element option

You can use this action to switch to the alternate Support Element when the primary fails. When the manual switchover action is started, the system checks that all internal code levels are the same and that the CPC is activated. If the switch can be made concurrently, the necessary files are passed between the

Support Elements, and the new primary Support Element is rebooted. If a disruptive switch is necessary, the CPC will be deactivated before completing the switch.

There are several conditions, when in progress, that will prevent a switchover:

- A mirroring task
- An internal code update
- A hard disk restore
- An engineering change.

The system automatically attempts a switchover for the following conditions:

- Primary Support Element has a serious hardware problem
- Primary Support Element detects a CPC status check
- Alternate Support Element detects a loss of communications to the primary over both the service network and the customer's LAN.

Note: To disable the automatic switchover, See the **Customize Console Services** task.

To switch to the alternate Support Element:

1. Open the **Alternate Support Element** task.

   The Alternate Support Element window displays.
2. Select the **Switch the Primary Support Element and the Alternate Support Element** radio button.
3. Click **OK** to perform the action.

Accessing the mirror the primary Support Element data to the alternate Support Element option

Notes:

- Mirroring is suppressed if the Support Element has service status enabled.
- Mirroring is suppressed if the alternate Support Element was loaded with a different CD-ROM from the primary Support Element.
- Mirroring is suppressed if the alternate Support Element is fenced because of an automatic switch.
- The primary Support Element is scheduled for automatic mirroring at 10 a.m. each day with a one-hour window for starting the operation. A record is added to the Support Element's event log to indicate the outcome of the operation.

This action mirrors Support Element data for the central processor complex (CPC). Mirroring Support Element data copies it from the CPC's primary Support Element to its alternate Support Element. By regularly mirroring Support Element data, you can help ensure that the alternate Support Element looks and works the same as the primary Support Element in case you need to switch to the alternate Support Element (for example, because of a hardware failure on the primary Support Element).

Ordinarily, Support Element data is mirrored automatically each day or when you install internal code changes through single step internal code changes, but you can use this action to mirror Support Element data immediately, at any time, and for any reason. The following are examples of when you would want to mirror Support Element data instead of waiting for the automatic mirroring default times:

- Licensed internal code changes
- Input/output configuration data set (IOCDS) changes
- Hardware configuration definition (HCD) changes
- Dynamic I/O changes
- Dynamic load address and parameter changes
- LPAR data
- Profile changes
- Lockout disruptive tasks

- Scheduled operations

To mirror the primary Support Element data:

1. Open the **Alternate Support Element** task.

   The Alternate Support Element window displays.
2. Select **Mirror the Primary Support Element data to the Alternate Support Element**.
3. Click **OK** to perform the action.

Accessing the query switch capabilities option

The query switch capability action provides a quick check of the communication path between the Support Elements, the status of the automatic switch action, and their status. You can use this action before attempting a switch to the alternate Support Element or for checking the status of the automatic switch action.

To query switch capabilities:

1. Open the **Alternate Support Element** task.

   The Alternate Support Element window displays.
2. Select **Query Switch capabilities**.
3. Click **OK** to perform the action.

Alternate Support Element

Use this window to confirm or cancel your request to mirror Support Element data for the selected central processor complex (CPC), switch the Primary Support Element data to the Alternate Support Element, query the switch capabilities, reset the fenced Alternate Support Element, or force disabled user interface switch to enabled (Alternate Support Element).

Mirror the Primary Support Element data to the Alternate Support Element

Mirroring Support Element data copies it from a CPC's Primary Support Element to its Alternate Support Element. By regularly mirroring Support Element data, you help ensure the Alternate Support Element will look and work the same as the Primary Support Element, should you ever need to switch to using the Alternate Support Element (due to a Primary Support Element hardware failure, for example).

Ordinarily, Support Element data is mirrored automatically each day. But you can use this window to mirror Support Element data immediately, at any time and for any reason. For example, you may want to mirror Support Element data immediately after installing internal code changes on the Primary Support Element, to ensure the Alternate Support Element is at the same internal code level right away (otherwise, the Alternate Support Element would remain at the previous internal code level until its daily, automatic mirroring occurred).

To begin mirroring Support Element data for the selected CPC, select **Mirror the Primary Support Element data to the Alternate Support Element**.

Note: The Primary Support Element's daily automatic mirroring is scheduled for 10 a.m. with a one hour window for starting the operation. A record is added to the Support Element's event log to indicate the outcome of the operation.

Switch the Primary Support Element and the Alternate Support Element

This action switches the role of the two Support Elements, so that the Primary Support Element becomes an Alternate Support Element and the Alternate Support Element becomes a Primary Support Element.

To make a request to switch from the Primary Support Element to the Alternate Support Element, (or from the Alternate Support Element to the Primary Support Element), select **Switch the Primary Support Element and the Alternate Support Element**. This request automatically determines what type of switch

it is, queries whether the switch is concurrent or disruptive, and displays the appropriate confirmation panel showing the switch information.

Query Switch Capabilities

This action provides the current switch status of the Alternate Support Element and whether or not the user interface switch, the user interface switch concurrency, or the automatic switch are enabled or disabled.

To see if different types of Switch requests (User Initiated or Automatic) are enabled or disabled, select **Query Switch Capabilities**. This request also displays the reasons why a Switch request has been disabled. If the User Initiated Switch is enabled, you are informed whether the type of switch is Concurrent or Disruptive. Generally, this option is only used if a switch did **not** occur as expected, or if you have a plan to periodically run this option to ensure that the alternate Support Element has no problems and is enabled for both types of switching.

Reset Fenced Alternate Support Element (due to Automatic Switchover)

To re-enable Automatic Switchover once data has been gathered from the Alternate Support Element after a previous Automatic Switchover, select **Reset Fenced Alternate Support Element (due to Automatic Switchover)**.

Force Disabled User Interface Switch to Enabled

To override the switch capabilities and make it possible to do a disruptive switch, select **Force Disabled User Interface Switch to Enabled**.

For example, if you receive an error while performing an Engineering Change (EC) upgrade on the Alternate Support Element, you may not be allowed to switch to the Primary Support Element. Use Force Disabled User Interface Switch to Enabled to override this.

When you have selected an action, you can proceed with any of the following:

OK
To perform the selected action, click **OK**.

Cancel
To close this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Switch Disabled

The switch disabled status occurs when:

- Support Element is fenced from the previous automatic switchover
- A status change occurred on the Primary Support Element and has not been communicated to the Alternate Support Element

Or, if any of the following is in progress:

- Mirroring
- EC upgrade
- Restore Critical Data
- Install/Activate or Remove/Activate

OK
To close the window, click **OK**.

Help
To display help for the current window, click **Help**.

Disruptive Switch

To use Disruptive Switch to switch the Primary Support Element to the Alternate Support Element, the system must be in an Initial Program Load (IML) complete state **and** the code levels of the Primary Support Element and Alternate Support Element must be different.

Switch Disruptive
To switch the Primary Support Element to the Alternate Support Element, click **Switch Disruptive**.

The system must be in an Initial Program Load (IML) complete state **and** the code levels of the Primary Support Element and Alternate Support Element must be different.

Cancel
To close this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Concurrent Switch

You can use Concurrent Switch to switch the Primary Support Element to the Alternate Support Element if the code levels of the Primary Support Element and Alternate Support Element are the same **or** if the system is not in an Initial Program Load (IML) complete state.

Switch Concurrently
To switch the Primary Support Element to the Alternate Support Element, click **Switch Concurrently**.

The system must **not** be in an Initial Program Load (IML) complete state **or** the code levels of the Primary Support Element and Alternate Support Element must be the same.

Cancel
To close this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Switch Capabilities

This window displays the current switch status of the Alternate Support Element and whether or not the user interface switch, the user interface switch concurrency, or the automatic switch are enabled or disabled.

OK
To close the window, click **OK**.

Help
To display help for the current window, click **Help**.

Reset Fenced Support Element Confirmation

An automatic switch has occurred because an error was detected by either the Primary or the Alternate Support Element. It is important to re-enable the second Support Element so it can be effectively used as an Alternate Support Element, but it is also important to capture any error data that may be on the current Alternate Support Element before resetting the fenced Support Element. This is because resetting the fenced Support Element will re-enable mirroring, which will overlay the data on the current Support Element.

To reset the fenced Support Element and allow the Alternate Support Element to be active again, click **Reset Fenced Support Element**.

Use Reset Fenced Support Element Confirmation to allow the Alternate Support Element to be active again. If you choose to continue, you must be sure you have performed the following:

- Copied the log files from both the Primary and Alternate Support Elements

- Run the diagnostics against the Alternate Support Element hardware
- And, verified that the customer wants to continue to have the Alternate Support Element Automatic Switchover feature enabled. If not, disable that feature.

Cancel
To close this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Force User Interface Switch Enabled Confirmation

The **Force User Interface Switch Enabled** option overrides the switch capabilities, allowing you to switch to the Alternate Support Element when the Primary Support Element cannot function. Click **Force User Interface Switch Enabled**, to enable the function.

For example, if you receive an error while performing an Engineering Change (EC) upgrade on the Primary Support Element, you may not be allowed to switch to the Alternate Support Element. Use **Force User Interface Switch Enabled** to override this.

Cancel
To close this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Analyze Internal Code

Accessing the Analyze Internal Code task

This task enables you to retrieve, delete, or view the Licensed Internal Code fix of the CPC and its Support Element.

To analyze console internal code:

1. Open the **Analyze Internal Code** task. The Analyze Internal Code Changes window is displayed.
2. Use the menu bar for the actions you want to perform on the internal code:
   - Selecting **File** allows you to choose to delete a selected code fix or choose to retrieve an MCF from removable media or an FTP site.
   - Selecting **Options** allows you to activate or deactivate an internal code fix.
   - Selecting **View** allows you to review the internal code fix information you are about to activate or lists the code fixes that have already been accepted.
3. When you have completed this task, select **File** from the menu bar, then click **Exit**.

Analyze Internal Code

Use this window to perform specific actions on selected internal code. Internal code fixes modify the Licensed Internal Code of the CPC and its Support Element. The actions you can perform on the internal code fixes include:

- Reviewing internal code fix information and content.
- Retrieving and deleting internal code fixes.
- Activating and deactivating internal code fixes.

You can perform actions on internal code fixes only at the direction of your support system.

Select one or more internal code fixes from the list, then select a choice from the menu bar.

Click **File**, then select the following:

- **Delete** to erase one or more selected temporary internal code fixes.
- **Retrieve MCF from Removable Media** to receive internal code fixes from removable media.

Note: If you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

- **Retrieve MCF from FTP site** to receive internal code fixes from an FTP site.
- **Exit** to end this task and return to the console workplace.

Click **Options**, then select the following:

- Activate Internal Code Fix to prepare one or more internal code fixes to replace corresponding Licensed Internal Code.

  Note: This option is not available when you are accessing this task with a user ID definition that is based on the *Service Representative* task roles.
- Deactivate Internal Code Fix to prepare to remove one or more internal code fixes, to restore the corresponding Licensed Internal Code.

  Notes:

  1. You can activate or deactivate on one or more internal code fixes.
  2. This option is not available when you are accessing this task with a user identification that is based on the *Service Representative* task roles.

You can activate or deactivate on one or more internal code fixes.

Click **View**, then select the following:

- Internal Code Fix Information to display the contents of the file and list the code modules provided in an internal code fix.

  Note: You can only view the information on a single code fix.
- **Accepted Internal Code Fixes** to list internal code fixes that are a permanent part of the Licensed Internal Code on the console. You do not need to select an internal code fix to use this choice. Accepted fixes are no longer available for use with menu choices. An internal code fix is accepted when its internal code change level is accepted.

Click **Help** to display help for the current window.

You can find more detailed help on the following elements of this window:

Change management services

Change management services control the availability of operations used to work on internal code change levels stored on the Support Element hard disk.

Change management services are either enabled or disabled, depending on the status of internal code fixes stored on the Support Element hard disk.

Enabled
Indicates you can work on internal code change levels stored on the Support Element hard disk. The required operations are available.

Disabled
Indicates you cannot work on internal code change levels stored on the Support Element hard disk. The required operations are not available.

The services become disabled to prevent the use of an internal code change level that differs, in any way, from the change level provided by the support system.

Internal code change levels may be altered unintentionally by errors that occur while copying them. For example, change levels may not be copied correctly from removable media to the Support Element hard disk.

Internal code change levels can be altered intentionally when you use the **Analyze Internal Code Change** window to activate a temporary internal code fix, or to activate individual fixes from a change level.

Note: If change management services are disabled, contact your support system for instructions before using the **Analyze Internal Code** task or the **Change Internal Code** task.

Internal code fixes table

This list displays the internal code fixes stored on the console hard disk. Select one or more fixes to work on, then select a choice from the menu bar.

EC Number
Specifies the Engineering Change (EC) number.

ID
Specifies the internal code fix identification.

Level
Identifies the internal code change level that includes the fix.

Note: Level 000 is not associated with an MCL.

Status
Indicates the outcome of the most recent work performed on the fix.

Date
Displays the date of the most recent change in status.

Time
Displays the time of day on the date of the most recent change in status.

Description
Displays a summary of engineering data or machine dependencies for the fix.

You can find more detailed help on the following:

Internal code fix status

The status of an internal code fix indicates the outcome of the most recent action performed on the fix. The status also indicates the type of action you can perform on the fix now. The status types and their conditions are the following:

Activated
The internal code fix is currently activated. The fix was activated individually using the **Analyze Internal Code Changes** window.

AutoActivated
The internal code fix is currently activated. The fix was activated automatically due to the activation of its internal code change level. The change level was activated by using the **Change Internal Code** task.

Deactivated
The internal code fix is currently deactivated. The internal code fix can be activated or viewed.

Error
An attempt to activate the internal code fix was not successful. The internal code fix is not activated.

Activated pending reboot
A request was made to activate the internal code fix, but the system requires a reboot.

Deactivated pending reboot
A request was made to deactivate the internal code fix, but the system requires a reboot.

Activate Internal Code Fix

To prepare one or more internal code fixes to replace corresponding licensed internal code, select **Activate Internal Code Fix**.

You must select one or more fixes to use with this choice.

The selected fixes are checked for syntax errors. The status of each fix becomes **Activated** or **Activated Pending Reboot** if no syntax errors are found.

If syntax errors are found in a fix, its status becomes **Error**. The fix must be edited to correct the errors before it can be activated.

This choice is available only while internal code fixes from the default directory display. Otherwise, it is unavailable.

Deactivate Internal Code Fix

To prepare to remove one or more internal code fixes and then restore the corresponding licensed internal code, select **Deactivate Internal Code Fix**.

You must select one or more fixes to use with this choice.

Deactivating internal code fixes does not erase them. The internal code fixes are replaced by corresponding licensed internal code. But the fixes remain available on the Support Element hard disk.

The status of each fix becomes **Deactivated** or **Deactivated pending reboot** upon selecting this option.

This choice is available only while internal code fixes from the default directory display. Otherwise, it is unavailable.

Internal Code Fix Information

This window displays the contents of the file (**Details** tab) and lists the code modules (**Modules** tab) provided in an internal code fix.

Click **Cancel** to close the window.

Click **Help** to display help for the current window.

Details

Licensed Internal Code, referred to also as internal code, controls many of the operations available on the CPCs and their Support Elements. Internal code changes may provide new internal code or correct or improve existing internal code.

A service representative will provide new internal code changes and manage their initial use.

File name
Displays the name of the internal code fix file. An internal code fix name is made up of the following information:

- A one-character internal code fix type identifier
- A six-character engineering change (EC) name
- A three-character sequence number.

When saved as an internal code fix file, the fix type identifier and the EC name are used for the file name and the sequence number is the file extension.

Level
Identifies the internal code change level that includes the fix.

Author
Displays the name of the person who wrote the internal code fix.

Status
Displays a description of the status of the fix.

Date of last update
Displays the date of the most recent change in status.

Time of last update
Displays the time of day on the date of the most recent change in status.

Description
Displays a summary of engineering data or machine dependencies for the internal code fix.

Modules

Use this window to view the modules table which displays a list of the internal code fix modules.

File Name
The name of the file as it will exist on the Support Element after the fix is activated.

Module Name
The name of the file as it exists in the Support Element.

Size
The number of bytes in the module.

Date
The date the module was created.

Time
The day and time the module was last updated.

Browse MCF Data

To view the contents of the selected MCF (microcode fix) data file, click **Browse MCF Data**.

Browse MCL Data

If an MCF is included in an MCL (microcode library) data file, you can view the contents of the selected MCL data file by clicking **Browse MCL Data**.

Audit and Log Management

Accessing the Audit and Log Management task

Use this task to choose the audit data types to be generated, viewed, and offloaded to a remote workstation or removable media.

To generate audit report data:

1. Open the **Audit and Log Management** task. The Audit and Log Management window is displayed.
2. Select the report type to be generated.
3. Select the audit data type of report you want to generate from the audit data types list.

   Note: The audit data types list displays only the data types that the user has authority to view.
4. Optionally, select **Limit event based audit data to a specific range of dates and times** to limit the report content for the selected event based audit data types to a time and date range.
5. Optionally, select the range of dates and times for the event based audit data types using the **View Calendar** and **View Time** icons to the right of the entry fields.
6. Click **OK** to generate the selected reports.

Audit and Log Management

Use this window to choose the audit data types to be generated, viewed, and offloaded to a remote workstation or removable media.

To generate an audit report:

- Select the report type to be generated
- Select the audit data type of report you want to generate from the **Audit data types** list

  Note: The audit data types list only displays the data types that the user has authority to view.
- Optionally select **Limit event based audit data to a specific range or dates and times** to limit the report content for the selected event based audit data types to a time and date range
- Optionally select the range of dates and times for the event based audit data types using the icons to the right of the entry fields

- Click **OK** to generate the report.

Additional functions on this window include:

OK
To proceed with your selections, click **OK**.

Cancel
To close this window and exit the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Report type

Select the format type of report to be generated. The supported types of reports are:

HTML
HyperText Markup Language is used to generate an easily viewable report.

XML
eXtensible Markup Language is used to generate a report that is easily parsed by programs for backend processing.

Note: You can view the XML schema file from Resource Link. This file defines the form of the XML output for audit, event, and security logs.

Range for event based audit data types

Use this section to limit the selected event based audit data type log to a specific range of dates and times. Use the **View Calendar** and **View Time** icons to the right of the entry fields to indicate the date and time for the selected event based audit data types to be included in the generated report.

Limit event based audit data to a specific range of dates and times
To limit the report content for the selected event based audit data types to a specific date and time range, select **Limit event based audit data to a specific range of dates and times**.

Starting date
Specify the starting date for the range used to limit the content of selected event based audit data types contained in the report. Use the icon to the right of the entry fields to indicate the starting date for the selected event based audit data types to be generated.

Starting time
Specify the starting time for the range used to limit the content of selected event based audit data types contained in the report. Use the icon to the right of the entry fields to indicate the starting time for the selected event based audit data types to be generated.

Ending date
Specify the ending date for the range used to limit the content of selected event based audit data types contained in the report. Use the icon to the right of the entry fields to indicate the ending date for the selected event based audit data types to be generated.

Ending time
Specify the ending time for the range used to limit the content of selected event based audit data types contained in the report. Use the icon to the right of the entry fields to indicate the ending time for the selected event based audit data types to be generated.

Audit data types

Select the audit data types that you want included in the audit report from the list. When you have completed selecting the preferred audit data types, click **OK** to generate the audit report. The Audit and Log Report window displays the audit report.

Note: The audit data types list only displays the data types that the user has authority to view. For example, the "Users" data type under "User profiles" is only shown to users who are authorized to the **Manage Users** task portion of the **User Management** task.

Audit and Log Report

Use this window to view a generated audit report and offload the generated report to a remote workstation or removable media.

Additional functions on this window include:

Save...

You can save the generated audit report:

Remotely
A browser window displays to specify the location for the audit report to be saved. To save the audit report content, click **Save...**.

Locally
A window displays to specify the name of the file and removable media selection for saving the audit report. To save the audit report content, click **Save...**.

Close
To close this window and return to the previous window, click **Close**.

Help
To display help for the current window, click **Help**.

Authorize Internal Code Changes

Accessing the Authorize Internal Code Changes task

When the internal code change authorization setting is enabled, you can use the Support Element console to install and activate internal code changes and to perform subsequent change management operations:

- Accept internal code changes to make them permanent internal code.
- Remove internal code changes to resolve problems.
- Delete internal code changes to attempt error recovery.

Normally, the setting is enabled, which allows changing the internal code of the system and its Support Element. You can manually disable the setting if there is any reason you do not want internal code to be changed.

The Support Element console also disables the setting automatically if it detects errors after activating new internal code changes, to prevent accepting the erroneous internal code changes. If this happens, you can manually enable the setting again when you want to install and activate new internal code changes that correct the previously detected error.

To change the setting for internal code change authorization:

1. Locate the CPC to work with.
2. Open the **Authorize Internal Code Changes** task.
3. Use the Authorize Internal Code Changes window controls to enable or disable the setting for internal code change authorization:
   a. While the setting is enabled, the **Do not allow installation and activation of internal code changes** check box is empty.

      To disable the setting of the next activation, click once on the check box to mark it.

   b. While the setting is disabled of the next activation, the **Do not allow installation and activation of internal code changes** check box displays a check mark.

      To enable the setting, click once on the check box to unmark it.

   c. Click **Save** to save the setting and close the window.

Authorize Internal Code Changes

Use this window to verify or change the setting that allows using this console to perform installation and activation of internal code changes and other **subsequent operations**.

When to change the setting

Normally, the operations are **allowed**.

- Change the setting to not allow the operations when you do not want internal code to be changed. This can be for any reason.
- Change the setting to not allow the operations when you perceive a problem after changes are activated. This prevents installing and activating the same changes on other systems, and reduces the risk of causing the same problem on them.
- Change the setting to allow the operations when you want to install and activate changes that correct a previously detected problem.

Notes:

- The console automatically changes the setting to not allow the operations if it detects errors after activating new internal code changes.
- The setting applies only to operations performed using this console.

Do not allow installation and activation of internal code changes
To change the setting that allows using this console to perform installation and activation of internal code changes and other **subsequent operations**, select **Do not allow installation and activation of internal code changes**.

A check mark displays to indicate the operations are **not allowed**.

Subsequent Operations

A set of tasks that can be used to work with internal code changes and a system only after the changes are installed or activated.

Subsequent operations include:

- Accepting changes that are installed and activated.
- Removing changes that are installed but not activated.
- Deleting changes that are removed, or retrieved but not installed.
- Backing up critical hard disk data.

The internal code change setting for a console controls whether performing the operations is allowed.

The option displays the current setting:

Select the option
A check mark is displayed and indicates the operations are **not allowed**.

Not allowed
An internal code change setting that does not allow using a console to perform installation and activation of internal code changes and other **subsequent operations**.

This is not the normal setting.

Normally, the operations are **allowed**.

The normal setting might be changed to not allow the operations:

- Manually, by a user who wants to prevent changing internal code for any reason.
- Automatically, by the console when it detects an error after activating new internal code changes.
- Manually, by a user who perceives a problem after activating new internal code changes.

Do not select the option
A check mark is not displayed and indicates the operations are **allowed**.

Allowed
An internal code change setting that allows using a console to perform installation and activation of internal code changes and other **subsequent operations**.

This setting allows scheduling the operations to perform them automatically and on a regular basis. It also allows manually performing the operations using console tasks.

This is the normal setting.

Select or clear the option to change the setting, then click **Save**, to save the new setting.

Save
To save a new setting or to keep the existing setting and begin the operation, click **Save**.

The **Authorize Internal Code Changes Progress** window is displayed, click **OK** to exit this window.

Reset
To restore the setting to its original choice, click **Reset**.

Cancel
To exit the window without applying any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Automatic Activation

Accessing the Automatic Activation task

Follow your local procedures for recovering from a power outage that is the result of a utility power failure. You may be able to speed recovery from such power outages by *enabling automatic activation* for the central processor complex (CPC). *Automatic activation* is a CPC setting that controls whether the CPC is activated automatically when power is restored following a utility power failure:

- When automatic activation is *enabled*, and a utility power failure occurs, the CPC is activated automatically when utility power is restored. The CPC is activated using the same reset profile used most recently to activate the CPC before the power outage.
- When automatic activation is *disabled*, and a utility power failure occurs, the CPC power remains off when utility power is restored. You can activate the CPC at any time, but manually, after utility power is restored.

To enable or disable automatic activation:

1. Open the Automatic Activation task.
2. Use the Customize Automatic Activation window's controls to enable or disable automatic activation:
   a. Select the CPC name from the list.
   b. Select **Options** from the menu bar.
   c. While automatic activation is disabled, select **Enable automatic activation** from the menu to change the CPC's setting to enabled.
   d. While automatic activation is enabled, select **Disable automatic activation** from the menu to change the CPC's setting to disabled.
   e. Click **Save** to save the setting and close the window.

Automatic Activation

Use this window to enable or disable automatic activation for the selected Central Processor Complex (CPC).

Automatic activation is a CPC setting that controls whether the selected CPC is activated automatically when power is restored following a utility failure.

You should customize the selected CPC's automatic activation setting, in advance, to suit your local procedures for recovering from a power outage that is the result of a utility power failure.

Activation table
Displays whether automatic activation is enabled or disabled and allows you to change the setting.

Object Name
Displays the name of the CPC.

Setting
Indicates whether automatic activation for the CPC is currently enabled or disabled.

- Enable Automatic Activation:

  To enable automatic activation for the selected CPC, select **Enabled**. When automatic activation is *enabled*, and a utility power failure occurs, the selected CPC is activated automatically when utility power is restored. The selected CPC is activated using the same reset profile used most recently to activate the CPC before the power outage.

- Disable Automatic Activation:

  To disable automatic activation for the selected CPC, select **Disabled**. When automatic activation is *disabled*, and a utility power failure occurs, the selected CPC power remains off when utility power is restored. You can manually activate the CPC at any time after utility power is restored.

Save
To save new settings, click **Save**.

Reset
To return to the settings from the last save, click **Reset**.

Cancel
To return to the settings from the last save and exit the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Enable Automatic Activation

To enable automatic activation for the selected Central Processor Complex (CPC) to automatically activate the last used reset profile:

1. Select the CPC. The selected CPC becomes highlighted and the setting for the selected is displayed.
2. Select **Enabled**. The automatic activation setting displays Enabled.
3. To save the setting, click **Save**. A message is displayed confirming that the setting is saved.
4. Click **OK**. The Automatic Activation window is displayed.
5. To return to the previous window without saving any more new settings, click **Cancel**.

Disable Automatic Activation

To disable automatic activation from the last used reset profile for the selected Central Processor Complex (CPC):

1. Select the CPC. The CPC becomes highlighted and the setting for the selected CPC is displayed.
2. Select **Disabled**. The automatic activation setting displays Disabled.
3. To save the setting, click **Save**. A message is displayed confirming that the setting is saved.
4. Click **OK**. The Automatic Activation window is displayed.
5. To return to the previous window without saving any more new settings, click **Cancel**.

Block Automatic Licensed Internal Code Change Installation

Accessing the Block Automatic Licensed Internal Code Change Installation task

This task, used by an access administrator or a user ID that is assigned access administrator roles, allows you to prevent automatically installed licensed internal code change from being installed outside of an explicitly initiated licensed internal code change installation operation.

Note: In most cases, this setting should not be changed. If this task is set to block automatic licensed internal code change installation, it prevents your system from automatically retrieving critical service or customer alerts, in addition to future enhanced driver maintenance sync port updates.

To block automatic licensed internal code change installation:

1. Open the **Block Automatic Licensed Internal Code Change Installation** task. The Block Automatic Licensed Internal Code Change Installation window is displayed.
2. Select **Block Automatic Licensed Internal Code Change Installation**, then click **Save** to complete the task.

Block Automatic Licensed Internal Code Change Installation

Use this window to prevent automatically installed licensed internal code changes from being installed outside of an explicitly initiated licensed internal code change installation operation.

When to change the setting

In most cases, this setting should not be changed. Blocking automatic licensed internal code change installation prevents your system from automatically retrieving Critical Service/Customer alerts, in addition to future Enhanced Driver Maintenance sync point updates.

To block automatically installed licensed internal code changes from being installed outside of an explicitly initiated licensed internal code change installation operation, select **Block automatic Licensed Internal Code Change installation**, then click **Save** to save the new setting.

Note: The setting applies only to licensed internal code changes for the current console.

Block automatic Licensed Internal Code Change installation
Changes the setting that blocks automatic licensed internal code change installation on this console.

The option displays the current setting if you:

Select the option
A check mark is displayed and indicates that automatic licensed internal code change installation is currently blocked.

Do not select the option
A check mark is NOT displayed and indicates that automatic licensed internal code change installation is currently blocked.

Save
To set the saved-state values to the changed setting choice and begin the operation, click **Save**.

Note: A message is displayed confirming your selection to block your system from automatically installing Critical Service/Customer alerts and future Enhanced Driver Maintenance sync point updates. Click **Yes** to continue or **No** to return to the previous window.

Cancel
To close this window and exit the task without applying any changes, click **Cancel**.

Note: If you click **Cancel** and made a change to this window without saving first, a message is displayed indicating a change has been made. Click **Yes** to exit the task without making changes, or click **No** to return to the previous window.

Help
To display help for the current window, click **Help**.

Change Internal Code

Change Internal Code

Use the **Change Internal Code** task to work with internal code changes for the console.

Licensed internal code, referred to also as internal code, controls many of the operations available on the console. Internal code changes may provide new internal code, or correct or improve existing internal code.

Note: A service representative will provide new internal code changes and manage their initial use. For internal code changes already stored on the console, it is recommended that you manage these changes only under the supervision of a service representative or with the assistance of the support system.

Working with internal code changes

Use the **Change Internal Code** task to start any of the following actions for working with the internal code changes.

It is recommended to take the following actions while following the internal code change process:

- Accept previous internal code changes to make them permanent internal code.
- Retrieve new internal code changes from a source to the console.
- Install and activate new internal code changes to make them operational.

Or use the following actions for undoing internal code changes:

- Remove internal code changes to resolve problems.
- Delete internal code changes to attempt error recovery.

Change Management Services

The status of change management services determines whether you can change internal code at this time, and controls the availability of applicable options for changing internal code.

The field displays **Enabled** to indicate you can change internal code at this time.

Concurrent Internal Code changes

The status of concurrent internal code changes is always enabled allowing the installation and activation of the changes with a power-on reset.

Select the option that describes the task you want to perform, then click **OK** to start the task.

Accept installed changes that were activated
To make operational internal code changes permanent, select **Accept installed changes that were activated**.

Check dependencies
To check whether internal code changes meet all the dependencies that must be met to use them with operations that change the internal code of the console, select **Check dependencies**.

Install and activate changes that were retrieved
To make retrieved internal code changes operational, select **Install and activate changes that were retrieved**.

Browse system and internal code information
To display information about the console and its internal code changes, select **Browse system and internal code information**.

Remove and activate changes
To undo the installation of installed internal code changes and to make their previous change levels operational, select **Remove and activate changes**.

Retrieve internal code changes
To copy internal code changes from a source to the console and to retrieve internal code changes from the support system to media, select **Retrieve internal code changes**.

Delete retrieved changes that were not installed
To erase retrieved internal code changes that are not yet installed or to erase removed internal code changes, select **Delete retrieved changes that were not installed**.

OK
To start the task that you have selected, click **OK**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Change Management Services

This field indicates the status of change management services on the console. The status of the services determines whether you can change internal code at this time, and controls the availability of applicable options for changing internal code.

Status indicators

Enabled
Indicates you can change internal code at this time. The applicable options for changing internal code are available.

Disabled
Indicates you cannot change internal code at this time. All options for changing internal code are unavailable.

Note: Options that do not change internal code remain available. For example, the **Retrieve internal code changes** option remains available while change management services are disabled.

When change management services are disabled

Change management services cannot be enabled or disabled directly. Instead, the console sets the status of change management services following any operation that involves internal code changes.

The console disables change management services to prevent you from using internal code changes that differ, in any way, from the changes provided to you.

Internal code changes may be altered unintentionally by errors that occur while retrieving them. For example, the changes may not be copied correctly from the source to the Support Element.

Note: If change management services are disabled following an unsuccessful attempt to retrieve internal code changes, try to retrieve the changes again. If the error occurs again, and change management services remain disabled, report the error to your service representative.

Internal code changes may be altered intentionally by your service representative. For example, your service representative may apply a temporary internal code change to modify internal code changes stored on the console.

Note: If change management services are disabled, yet no errors have occurred, the disabled condition may be due to the use of a temporary internal code change. Your service representative must deactivate the temporary internal code change to enable change management services.

Accept installed changes that were activated

To make operational internal code changes permanent, select **Accept installed changes that were activated**.

Then click **OK** to start the task.

Consequences of using this option

Operational internal code changes include all installed changes that are currently activated.

Accepting operational internal code changes permanently changes the internal code of the console. Accepting the changes makes them internal code.

Accepting internal code changes cannot be undone. That is, accepted changes cannot be removed or deleted, and the internal code they changed cannot be restored.

Options for accepted changes

All options for changing internal code are no longer applicable to accepted internal code changes.

Availability of this option

This option is available while:

- Change management services are enabled.
- And one or more internal code changes are installed and currently activated.

Otherwise, the option is unavailable.

Check dependencies

To check whether internal code changes meet all the dependencies that must be met to use them with operations that change the internal code of the console, select **Check dependencies**.

Then click **OK** to start the task.

Note: Ordinarily, only a service representative checks the dependencies of internal code changes, typically while following a service procedure for changing the console's internal code. If you are not following a service procedure, it is recommended that you check dependencies only with assistance from product support, provided through your service representative or support system.

About internal code change dependencies

Internal code is organized into units called *Engineering Changes (ECs)*, which are also referred to as *streams*.

Internal code changes may provide new internal code, or correct or improve existing internal code, for particular streams. If internal code changes for multiple streams are needed, together, to complete an addition, correction, or improvement of the console's internal code, then the internal code changes have *dependencies*. For example, if Engineering Change (EC) E12345, change level 001, must be installed and activated before EC E54321 level 005 can be installed and activated, then EC E54321 level 005 has a dependency on EC E12345 level 001.

The dependencies of internal code changes are designated by when the changes are created. After internal code changes are retrieved to the console, their dependencies, if any, are checked automatically whenever you start an operation that will change the console's internal code. Such an operation will be attempted only if all dependencies of the internal code changes are met.

Manually checking dependencies

This option provides a means for manually checking the dependencies of internal code changes. Manually checking dependencies is useful:

- Before you perform an operation for changing the console's internal code.

  By manually checking the dependencies of internal code changes you intend to select while performing the operation, you may get a detailed list of the dependencies that would not be met, but which you must meet before or while actually attempting the operation.

Note: This is especially important if you intend to use specific internal code changes, rather than all changes, while performing the operation. Using specific changes increases the possibility of **not** specifying one or more dependencies of the specific changes.

- After automatic dependency checking notifies you, upon attempting an operation, that one or more dependencies are not met.

  By manually checking the dependencies of internal code changes you selected while attempting the operation, you get a detailed list of the dependencies that were not met, but which you must meet before or while attempting the operation again.

Availability of this option

This option is available while:

- Change management services are enabled.
- And one or more internal code changes are eligible for being either accepted, installed, or removed.

Otherwise, the option is unavailable.

Install and activate changes that were retrieved

To make retrieved internal code changes operational, select **Install and activate changes that were retrieved**.

Then click **OK** to start the task.

Consequences of using this option

Installing retrieved internal code changes makes them eligible for being activated. Activating installed changes makes them operational.

But installing and activating internal code changes does **not** permanently change the internal code of the console. Instead, installing changes makes them only temporarily eligible for being activated. Then activating the installed changes now, and any subsequent activation of the console, makes the changes operational instead of the internal code they changed.

Installed changes can be removed, if necessary, to restore the internal code they changed.

Options for installed and activated changes

After you install and activate internal code changes, the following options for changing internal code are applicable to them:

- Accept installed changes that were activated

  Use this option to make operational internal code changes permanent.
- Remove and activate changes

  Use this option to undo the installation of installed internal code changes and to make their previous change levels operational.

Availability of this option

This option is available while:

- Change management services are enabled.
- And one or more internal code changes are retrieved or removed.

Otherwise, the option is unavailable.

Browse system and internal code information

To display information about the console and its internal code changes, select **Browse system and internal code information**.

Then click **OK** to start the task.

About the information

Information about the console identifies its machine type, model number, and serial number.

Information about the internal code changes is a record of tasks performed on the changes. For each internal code change, the information identifies:

- Its Engineering Change (EC) number.
- The change level most recently retrieved.
- The change level most recently installed.
- The change level most recently activated.
- The change level most recently accepted.
- The lowest change level that can be activated after removing installed change levels.
- Additional details include the date and time each task was most recently performed.

Using the information

The information may assist you with planning and managing internal code changes. For example, review the information to either:

- Determine whether the console is operating with your latest available change levels.
- Determine which tasks you must perform next to make the console operate with your latest available change levels.

Remove and activate changes

To undo the installation of installed internal code changes and to make their previous change levels operational, select **Remove and activate changes**.

Then click **OK** to start the task.

Consequences of using this option

Removing installed internal code changes makes them ineligible for being activated, and makes their previous change levels eligible instead. Activating the previous change levels makes them operational.

But removing internal code changes and activating previous change levels does **not** permanently change the internal code of the console. Instead, removing changes restores the internal code they changed. Then activating without the removed changes now, and any subsequent activation of the console, makes the restored internal code operational.

Removed changes are not erased. They remain stored on the console and can be installed again at any time.

Options for removed changes

After you remove internal code changes, the following options for changing internal code are applicable to them:

- Install and activate changes that were retrieved

  Use this option to make removed internal code changes operational again.
- Delete retrieved changes that were not installed

Use this option to erase removed internal code changes if an error occurred while installing or activating them.

Availability of this option

This option is available while:

- Change management services are enabled.
- And one or more internal code changes are installed.

Otherwise, the option is unavailable.

Retrieve internal code changes

To copy internal code changes from a source to the console and to retrieve internal code changes from the support system to media, select **Retrieve internal code changes**.

Then click **OK** to start the task.

Consequences of using this option

Retrieving internal code changes makes them available for being installed and activated.

But retrieving internal code changes does **not** change the internal code of the console. It only copies them from their source to the console.

Options for retrieved changes

After you retrieve internal code changes, the following options for changing internal code are applicable to them:

- Install and activate changes that were retrieved

  Use this option to make retrieved internal code changes operational.
- Delete retrieved changes that were not installed

  Use this option to erase retrieved internal code changes if an error occurred while retrieving them.

Delete retrieved changes that were not installed

To erase retrieved internal code changes that are not yet installed and to erase removed internal code changes, select **Delete retrieved changes that were not installed**.

Then click **OK** to start the task.

Delete retrieved internal code changes if an error occurred while retrieving them. Remove then delete installed internal code changes if an error occurred while installing or activating them.

Consequences of using this option

Deleting internal code changes allows retrieving the changes over again if errors occurred during previous attempts to retrieve, install, or activate the changes.

Deleting internal code changes does **not** change the internal code of the console; it erases only retrieved and removed internal code changes from the console.

Options for deleted changes

All options for changing internal code are no longer applicable to deleted internal code changes. But if the source of the internal code changes is still available, the following option for changing internal code is applicable to them:

- Retrieve internal code changes

Use this option to copy internal code changes again from the source to the console.

Availability of this option

This option is available while:

- Change management services are enabled.
- And one or more internal code changes are retrieved or removed.

Otherwise, the option is unavailable.

Activate Internal Code Change Confirmation

Use this window to activate the internal code changes that are currently installed on the console.

Yes
To activate the internal code changes that are currently installed on the console, click **Yes**.

No
If you do not want to activate the internal code changes that are currently installed on the console, click **No**.

Help
To display help for the current window, click **Help**.

Specify Internal Code Changes

Use this window to identify the specific internal code changes you want the task you selected to apply to.

Identify the changes by their Engineering Change (EC) numbers and change levels.

Note: You will need the assistance of your service representative or your support system to identify a specific internal code change by its EC number and change level.

Engineering Change table
Complete one row of fields for each internal code change you want to apply the task to, then click **OK** to continue the task.

Note: Fields are initialized with default entries for EC numbers and change levels derived from previous entries, if any. If you do not want to use the default entries, click **Clear** to discard them. All entry fields will be cleared to allow you to specify other EC numbers and change levels.

EC Number
Specify the EC number of the internal code change you want the task you selected to apply to.

Then use the applicable fields in the same row to identify the change levels of the internal code change you want the task to apply to.

Starting Change Level and Ending Change Level
Enter the numbers of the first and last change levels you want to retrieve from the support system to a removable media. Or enter the starting change level, then enter **ALL** for the ending change level to retrieve all change levels.

The task will retrieve the specified range of change levels of the internal code changes identified by the adjacent EC number.

OK
To continue the selected action and apply it to the specific internal code changes identified by the EC numbers and change levels, click **OK**.

Clear
To remove all entry fields on the window by discarding the EC numbers and change levels specified the last time the window was used, click **Clear**.

Cancel

To close the window and return to the window from which you selected the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Specify Internal Code Changes

Use this window to identify the specific internal code changes you want the task you selected to apply to.

Identify the changes by their Engineering Change (EC) numbers and change levels.

Note: You will need the assistance of your service representative or your support system to identify a specific internal code change by its EC number and change level.

Select the type of operation
If you chose to **Remove and activate changes** or **Install and activate changes that were retrieved** then you can choose the type of operation you prefer by selecting **Do the changes concurrently** or **Do the changes disruptively**.

Engineering Change table
Complete one row of fields for each internal code change you want to apply the task to, then click **OK** to continue the task.

Note: Fields are initialized with default entries for EC numbers and change levels derived from previous entries, if any. If you do not want to use the default entries, click **Clear** to discard them. All entry fields will be cleared to allow entering other EC numbers and change levels.

EC Number
Enter the EC number of the internal code change you want the task you selected to apply to.

Then use the applicable field in the same row to identify the change levels of the internal code change you want the task to apply to.

Change Level
Specify the number of the last change level you want the task you selected to apply to, or enter **ALL** to apply the selected task to all applicable change levels.

The task will be applied to applicable change levels of the internal code change, identified by the adjacent EC number, from the current applicable change level to the change level you specify.

The applicable change levels and their range depends on the action you selected:

Accept
Applies to installed and activated change levels in the range from the lowest change level up to and including the change level you specify.

Check dependencies: Accept
Applies to installed and activated change levels in the range from the lowest change level up to and including the change level you specify.

Check dependencies: Install
Applies to retrieved change levels in the range from the lowest change level up to and including the change level you specify.

Check dependencies: Remove
Applies to installed change levels in the range from the highest change level down to and including the change level you specify.

Delete
Applies to retrieved and removed change levels in the range from the highest change level down to and including the change level you specify.

Install
Applies to retrieved change levels in the range from the lowest change level up to and including the change level you specify.

Remove
Applies to installed change levels in the range from the highest change level down to and including the change level you specify.

Retrieve
Applies to change levels available from the source in the range from the lowest change level up to and including the change level you specify.

Note: You will need the assistance of your service representative or your support system to identify a specific internal code change by its EC number and change level.

Include internal code changes which will inhibit the Concurrent Upgrade Engineering Changes (EC) task from being used to apply the next Licensed Internal Code EC level
This option is only available if you chose to **Install and activate changes that were retrieved** and if there are retrieved changes that would break the **Concurrent Upgrade Engineering Changes** task's maximum change level requirements if the changes were installed.

OK
To continue the selected task and apply it to the specific internal code changes identified by the EC numbers and change levels, click **OK**.

Clear
To remove all entry fields on the window by discarding the EC numbers and change levels specified the last time the window was used, click **Clear**.

Cancel

To close the window and return to the window from which you selected the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Select Internal Code Changes

Use this window to indicate whether you want the task you selected to apply to all or a subset of its applicable internal code changes.

Ordinarily, you should use all applicable internal code changes each time you use any task that changes the internal code. But you can use subsets of changes instead, if it meets your particular circumstances or needs for changing the internal code. For example, you may want to use specific changes:

- To install only some changes, but not other changes, to preserve internal code you do not want to change.
- To remove only some changes if they caused problems or did not operate satisfactorily, while letting other changes remain installed.

Important: It is recommended that you use specific internal code changes only under the supervision of a service representative or with the assistance of the support system.

All internal code changes
To apply the selected task to all its applicable internal code changes, select **All internal code changes**.

Specific internal code changes
To apply the selected task to a subset of its applicable internal code changes, select **Specific internal code changes**.

Then, on the subsequent window, identify the changes by their Engineering Change (EC) numbers and change levels.

Note: You will need the assistance of your service representative or your support system to identify specific changes.

Bundle of internal code changes
To apply a specified bundle level number for internal code changes, select **Bundle of internal code changes**.

OK
To continue the selected task and apply it to the internal code changes described by your selection, click **OK**.

Cancel
To close the window and return to the window from which you selected the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Check Dependencies Failed

This window indicates one or more dependencies were not met for using the selected operation and internal code changes to change the internal code of the console. The window also lists messages that describe each dependency that was not met. Each message includes:

- A description of the dependency.
- The operation you must perform to meet the dependency.
- The Engineering Change (EC) number and change level of each internal code change you can or must use with the operation to meet the dependency.

Upon returning to the service procedure you are following, you can proceed with its instructions and refer to its recovery actions for meeting failed dependencies described by the messages.

Important: Ordinarily, only a service representative checks the dependencies of internal code changes, typically while following a service procedure for changing the console's internal code. If you are not following a service procedure, it is recommended that you check dependencies only with assistance from product support, provided through your service representative or support system.

Engineering Change table
These entries indicate that one or more dependencies were not met for using the selected operation and internal code changes to change the internal code of the console.

OK
To return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

Check Dependencies

Use this window to check whether internal code changes meet all the dependencies that must be met to use them with operations that change the internal code of the console.

Note: Ordinarily, only a service representative checks the dependencies of internal code changes, typically while following a service procedure for changing the console's internal code. If you are not following a service procedure, it is recommended that you check dependencies only with assistance from product support, provided through your service representative or support system.

Internal code is organized into units call *Engineering Changes (ECs)*, which are referred to also as *streams*.

Internal code changes may provide new internal code, or correct or improve existing internal code, for particular streams. If internal code changes for multiple streams are needed, together, to complete an addition, correction, or improvement of the console's internal code, then the internal code changes have *dependencies*. For example, if Engineering Change (EC) E12345, change level 001, must be installed and activated before EC E54321 level 005 can be installed and activated, then EC E54321 level 005 has a dependency on EC E12345 level 001.

The dependencies of internal code changes are designated by when the changes are created. After internal code changes are retrieved to the console, their dependencies, if any, are checked automatically whenever you start an operation that will change the console's internal code. Such an operation will be attempted only if all dependencies of the internal code changes are met.

This option provides a means for manually checking the dependencies of internal code changes. Manually checking dependencies is useful:

- Before you perform an operation for changing the console's internal code.

By manually checking the dependencies of internal code changes you intend to select while performing the operation, you may get a detailed list of the dependencies that would not be met, but which you must meet before or while actually attempting the operation.

Note: This is especially important if you intend to use specific internal code changes, rather than all changes, while performing the operation. Using specific changes increases the possibility of not specifying one or more dependencies of the specific changes.

- After automatic dependency checking notifies you, upon attempting an operation, that one or more dependencies are not met.

  By manually checking the dependencies of internal code changes you selected while attempting the operation, you get a detailed list of the dependencies that were not met, but which you must meet before or while attempting the operation again.

Dependency checking options

To check dependencies of internal code changes manually, select the option that describes the operation and internal code changes for which you want dependencies checked, then click **OK**.

Install and activate of all changes
To check the dependencies that must be met to install and activate all internal code changes, select **Install and activate of all changes**.

Remove and activate of all changes
To check the dependencies that must be met to remove and activate all internal code changes, select **Remove and activate of all changes**.

Install and activate of specific changes
To check the dependencies that must be met to install and activate specific internal code changes, select **Install and activate of specific changes**.

Remove and activate of specific changes
To check the dependencies that must be met to remove and activate specific internal code changes, select **Remove and activate of specific changes**.

Accept specific changes
To check the dependencies that must be met to accept specific internal code changes, select **Accept specific changes**.

OK
To start the dependency checking described by your selection, click **OK**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Install and activate of all changes

To check the dependencies that must be met to install and activate all internal code changes, select **Install and activate of all changes**.

Automatic dependency checking is performed when you actually attempt to change the internal code of the console by installing and activating all internal code changes. But you can use this choice to manually perform the same dependency checking now, without installing and activating the changes or otherwise changing the console's internal code.

Changes checked for dependencies

Selecting this choice checks that dependencies of only the internal code changes that are eligible for being installed and activated. That is, dependencies will be checked only for internal code changes that were retrieved to the console, but are not currently installed.

Using the results of dependency checking

The results of dependency checking provide information that may assist you with planning and managing internal code changes. For example:

- If the results indicate all dependencies are met, you can proceed with actually installing and activating all internal code changes.
- If the results indicate not all dependencies are met, you can use the detailed information provided in the results to meet the dependencies before or while actually installing and activating all internal code changes.

  Note: The detailed information identifies the operations and internal code changes you must use to meet the dependencies.

Availability of this option

This option is available while internal code changes are eligible for being installed. That is, this option is available while any changes are retrieved.

Otherwise, the option is unavailable.

Remove and activate of all changes

To check the dependencies that must be met to remove and activate all internal code changes, select **Remove and activate of all changes**.

Automatic dependency checking is performed when you actually attempt to change the internal code of the console by removing and activating all internal code changes. But you can use this choice to manually perform the same dependency checking now, without removing and activating the changes or otherwise changing the console's internal code.

Changes checked for dependencies

Selecting this choice checks that dependencies of only the internal code changes that are eligible for being removed and activated. That is, dependencies will be checked only for internal code changes that are currently installed.

Using the results of dependency checking

The results of dependency checking provide information that may assist you with planning and managing internal code changes. For example:

- If the results indicate all dependencies are met, you can proceed with actually removing and activating all internal code changes.
- If the results indicate not all dependencies are met, you can use the detailed information provided in the results to meet the dependencies before or while actually removing and activating all internal code changes.

  Note: The detailed information identifies the operations and internal code changes you must use to meet the dependencies.

Availability of this option

This option is available while internal code changes are eligible for being removed. That is, this option is available while any changes are retrieved.

Otherwise, the option is unavailable.

Install and activate of specific changes

To check the dependencies that must be met to install and activate specific internal code changes, select **Install and activate of specific changes**.

Automatic dependency checking is performed when you actually attempt to change the internal code of the console by installing and activating specific internal code changes. But you can use this choice to manually perform the same dependency checking now, without installing and activating the changes or otherwise changing the console's internal code.

Changes checked for dependencies

Selecting this choice checks that dependencies of only the internal code changes you specify on a subsequent window, if the changes are eligible for being installed and activated. That is, dependencies will be checked only for specified internal code changes that were retrieved to the console, but are not currently installed.

Using the results of dependency checking

The results of dependency checking provide information that may assist you with planning and managing internal code changes. For example:

- If the results indicate all dependencies are met, you can proceed with actually installing and activating the specific internal code changes.
- If the results indicate not all dependencies are met, you can use the detailed information provided in the results to meet the dependencies before or while actually installing and activating the specific internal code changes.

  Note: The detailed information identifies the operations and internal code changes you must use to meet the dependencies.

  Important: Many combinations of specific internal code changes may meet all dependencies for being installed and activated, but it is recommended that you install and activate all retrieved internal code changes instead. Using specific changes risks installing and activating an untested combination of changes.

Availability of this option

This option is available while any internal code changes are eligible for being installed. That is, this option is available while any changes are retrieved.

Otherwise, the option is unavailable.

Remove and activate of specific changes

To check the dependencies that must be met to remove and activate specific internal code changes, select **Remove and activate of specific changes**.

Automatic dependency checking is performed when you actually attempt to change the internal code of the console by removing and activating specific internal code changes. But you can use this choice to manually perform the same dependency checking now, without installing and activating the changes or otherwise changing the console's internal code.

Changes checked for dependencies

Selecting this choice checks that dependencies of only the internal code changes you specify on a subsequent window, if the changes are eligible for being removed and activated. That is, dependencies will be checked only for specified internal code changes that are currently installed.

Using the results of dependency checking

The results of dependency checking provide information that may assist you with planning and managing internal code changes. For example:

- If the results indicate all dependencies are met, you can proceed with actually removing and activating the specific internal code changes.

- If the results indicate not all dependencies are met, you can use the detailed information provided in the results to meet the dependencies before or while actually removing and activating the specific internal code changes.

  Note: The detailed information identifies the operations and internal code changes you must use to meet the dependencies.

  Important: Many combinations of specific internal code changes may meet all dependencies for being removed and activated, but it is recommended that you remove and activate all installed internal code changes instead. Using specific changes risks removing and activating an untested combination of changes.

Availability of this option

This option is available while any internal code changes are eligible for being removed. That is, this option is available while any changes are installed.

Otherwise, the option is unavailable.

Accept specific changes

To check the dependencies that must be met to accept specific internal code changes, select **Accept specific changes**.

Automatic dependency checking is performed when you actually attempt to change the internal code of the console by accepting specific internal code changes. But you can use this choice to manually perform the same dependency checking now, without accepting the changes or otherwise changing the console's internal code.

Changes checked for dependencies

Selecting this choice checks that dependencies of only the internal code changes you specify on a subsequent window, if the changes are eligible for being accepted. That is, dependencies will be checked only for specified internal code changes that are currently installed and activated.

Using the results of dependency checking

The results of dependency checking provide information that may assist you with planning and managing internal code changes. For example:

- If the results indicate all dependencies are met, you can proceed with actually accepting the specific internal code changes.
- If the results indicate not all dependencies are met, you can use the detailed information provided in the results to meet the dependencies before or while actually accepting the specific internal code changes.

  Note: The detailed information identifies the operations and internal code changes you must use to meet the dependencies.

  Important: Many combinations of specific internal code changes may meet all dependencies for being accepted, but it is recommended that you accept all installed and activated internal code changes instead. Using specific changes risks accepting an untested combination of changes.

Availability of this option

This option is available while any internal code changes are eligible for being accepted. That is, this option is available while any changes are installed and activated.

Otherwise, the option is unavailable.

Retrieve Internal Code Changes

Use this window to copy internal code changes from their source to the console.

Retrieve Internal Code Changes options

Select the option that describes the action you want to perform, then click **OK** to start the action.

Retrieve code changes from removable media to the console
To copy internal code change from removable media to the console, select **Retrieve code changes from removable media to the console**.

Retrieve code changes from the support system to the console
To copy internal code changes from the support system to the console, select **Retrieve code changes from the support system to the console**.

Retrieve code changes from FTP site to the console
To copy internal code changes from a designated FTP site to the console, select **Retrieve code changes from FTP site to the console**.

OK
To start the task that you selected, click **OK**.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Retrieve code changes from removable media to the console

To copy internal code changes from removable media, select **Retrieve code changes from removable media to the console**.

Note: When you use a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

Use this option when you have removable media that has internal code changes stored on it. For example, use this option when either:

- The support system has delivered the internal code changes to you on removable media.
- You used another console to copy internal code changes from the support system to removable media.

Retrieve code changes from the support system to the console

To copy internal code changes from the support system to the console, select **Retrieve code changes from the support system to the console**.

Use this option when:

- This console is configured and enabled for communicating with the support system.
- And after you are notified that new internal code changes are available from the support system.

Retrieve code changes from FTP site to the console

To copy internal code changes from an FTP site to the console, select **Retrieve code changes from FTP site to the console**.

This option allows you to enter the FTP site address and account access information.

FTP Server Information / Configure Backup Settings

Use this window to configure FTP settings when you use an external server to back up your files or when you are transferring data for the following tasks:

- Analyze Console Internal Code

- Change Console Internal Code
- Retrieve Internal Code (targeting an object)
- Backup Critical Data
- Save Upgrade Data

Host name
Specify the host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

OK
To apply this information, click **OK**.

Clear
To remove all information from the input fields, click **Clear**.

Cancel
To close the window without providing information, click **Cancel**.

Help
To display help for the current window, click **Help**.

Confirm the Action: Accept

Use this window to confirm or cancel your request to accept operational internal code changes.

Accepting operational internal code changes makes them permanent internal code.

At this point in the task, **operational internal code changes** are:

- All changes you installed that are currently activated.
- But limited to the set of changes you selected for the task on a previous window: either all changes or specific changes.

Attention: Accepting internal code changes permanently changes the internal code of the console. The process cannot be undone. That is, accepted internal code changes cannot be removed to restore their previous change levels.

Internal code change process

The window displays the summary of the internal code change process that are recommended. Accepting internal code changes is the second step (step **B**) of the process. Review the process before continuing.

Note: You should cancel your request to accept internal code changes in these cases:

- If you have not completed the third or fourth steps (steps **C** or **D**) of the process for **previous** internal code changes. That is:
  - If you have not yet retrieved all **previous** internal code changes provided to you by the support system.
  - Or if you did not install and activate the previously retrieved internal code changes after checking their dependencies.
- Or if you have not completed the first step (step **A**) of the internal code change process upon receiving new internal code changes. That is, if you have not yet performed a backup of critical data of the console.

You should confirm your request to accept internal code changes only after completing the recommended steps described above.

Accept
To confirm your request to accept operational internal code changes, click **Accept**.

Cancel
To cancel your request and close the window without accepting the operational changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Confirm the Action: Retrieve from a source to console

Use this window to confirm or cancel your request to retrieve internal code changes from their source to the console.

Retrieving internal code changes makes them available for being installed and activated.

At this point in the task, **internal code changes** are:

- All changes available from the source you selected.
- But limited to the set of changes you selected for the task on a previous window: either all changes or specific changes.

Internal code change process

The window displays a summary of the internal code change process. Retrieving internal code changes is the third step (step **C**) of the process. Review the process before continuing.

Note: You should cancel your request to retrieve internal code changes in these cases:

- If you have not completed the last step (step **D**) of the process for **previous** internal code changes. That is, if you have not yet installed and activated all **previously** retrieved internal code changes.
- If you did not perform the first or second steps (steps **A** or **B**) of the process upon receiving the new internal code changes. That is:
  - If you have not yet performed a backup of critical data of the console.
  - Or if you have not yet accepted all **previously** installed and activated internal code changes.

You should confirm your request to retrieve new internal code changes only after completing the recommended steps described above.

Retrieve
To confirm your request to retrieve internal code changes from their source to the console, click **Retrieve**.

Cancel
To cancel your request and close the window without retrieving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Confirm the Action: Retrieve from a support system to console

Use this window to confirm or cancel your request to retrieve internal code changes from their source to the console.

Retrieving internal code changes makes them available for being installed and activated.

At this point in the task, **internal code changes** are:

- All changes available from the source you selected.
- But limited to the set of changes you selected for the task on a previous window: either all changes or specific changes.

Internal code change process

The window displays a summary of the recommended internal code change process. Retrieving internal code changes is the third step (step **C**) of the process. Review the process before continuing.

Note: You should cancel your request to retrieve internal code changes in these cases:

- If you have not completed the last step (step **D**) of the process for **previous** internal code changes. That is, if you have not yet installed and activated all **previously** retrieved internal code changes.
- If you did not perform the first or second steps (steps **A** or **B**) of the process upon receiving the new internal code changes. That is:
  - If you have not yet performed a backup of critical data of the console.
  - Or if you have not yet accepted all **previously** installed and activated internal code changes.

You should confirm your request to retrieve new internal code changes only after completing the recommended steps described above.

Retrieve
To confirm your request to retrieve internal code changes from their source to the console, click **Retrieve**.

Cancel
To cancel your request and close the window without retrieving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Confirm the Action: Install and Activate

Use this window to confirm or cancel your request to install and activate the retrieved internal code changes.

Installing and activating the retrieved changes makes them operational.

At this point in the task, **retrieved internal code changes** are:

- All changes you retrieved from their source to the console. That is, all changes that are eligible for being installed.
- But limited to the set of changes you selected for the task on a previous window: either all changes or specific changes.

Internal code change process

The window displays a summary of the internal code recommended change process. Installing and activating internal code changes is the last step (step **D**) of the process. Review the process before continuing.

Important: You should cancel your request to install and activate internal code changes if you did not perform the preceding steps (steps **A** through **C**) of the process upon receiving the new internal code changes. That is:

- If you have not yet performed a backup of critical data of the console.
- Or if you have not yet accepted all **previously** installed and activated internal code changes.
- Or if you have not yet retrieved the new internal code changes provided to you by the support system.

You should confirm your request to install and activate new internal code changes only after completing the recommended steps described above.

Install and Activate
To confirm your request to install and activate the retrieved internal code changes, click **Install and Activate**.

Cancel
To cancel your request, and close the window without installing or activating the retrieved changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Confirm the Action: Remove and Activate

Use this window to confirm or cancel your request to remove the installed internal code changes and to activate their previous change levels.

Removing the installed changes and activating their previous change levels makes the previous levels operational. Any subsequent initialization of the console also will make the previous change levels operational.

At this point in the task, **installed internal code changes** are:

- All changes you installed, but have not yet accepted or removed. That is, all changes that are activated or eligible for being activated.
- But limited to the set of changes you selected for the task on a previous window: either all changes or specific changes.

Remove and Activate
To confirm your request to remove and activate the installed internal code changes, click **Remove and Activate**.

Cancel
To cancel your request, and close the window without removing the installed changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Confirm the Action: Delete

Use this window to confirm or cancel your request to delete:

- Retrieved internal code changes.
- Removed internal code changes.

At this point in the task:

- **Retrieved internal code changes** are all changes you retrieved from their source to the console, but have not yet installed.
- And **removed internal code changes** are all retrieved changes you installed, but then removed to undo their installation.
- But both are limited to the set of changes you selected for the task on a previous window: either all changes or specific changes.

Important: Deleting internal code changes erases them from the console. The process cannot be undone. However, deleted internal code changes can be retrieved again from their source to the console.

Delete
To confirm your request and delete the internal code changes, click **Delete**.

Cancel
To cancel your request, and close the window without deleting the internal code changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Specify Bundle to Install

Use this window to provide a bundle level number that you want installed.

Bundle Level
Specify the bundle level number in the input area.

OK
To proceed with installing the specified bundle level number, click **OK**.

Cancel

To return to the previous window without providing a bundle level number, click **Cancel**.

Help
To display help for the current window, click **Help**.

Change LPAR Controls

Accessing the Change LPAR Controls task

Note: This task is not available when one or more managed systems have DPM enabled.

The settings that determine how processor resources are assigned to, used by, and managed for logical partitions that can be activated on the central processor complex (CPC) are referred to here as *control settings*. More specifically, control settings determine:

- Whether logical partitions are assigned dedicated or shared processor resources.
- How each logical partition activated with shared processor resources shares them with other logical partitions activated with shared processor resources.
- How the CPC manages logical partitions' use of shared processor resources.

Both the CPC and its logical partitions have control settings. A logical partition's control settings apply to it only. The CPC's control settings apply to all of its logical partitions. The control settings are:

Logical processor assignment
These logical partition settings control how many logical processors are assigned to the logical partition, how they are assigned as either dedicated or shared processor resources, the processing weights, and absolute capping of logical partitions. The settings control how a partition is workload managed and whether software pricing is to change based on the number of defined capacity.

Processor running time
These CPC settings control how its logical partitions' processor running time is determined. The processor running time, referred to also as a timeslice, is the amount of continuous time allowed for each logical partition's logical processors to perform jobs on shared central processors.

The initial control settings of the CPC and each logical partition are established by the activation profiles used to activate them. See the following topics for more information about customizing activation profiles for establishing initial control settings:

- Activation profiles
- Assigning initial logical or reserved processors

- Setting processor running time
- Setting defined capacity
- Setting Workload Manager (WLM) controls

To review or change control settings:

1. Open the **Change LPAR Controls** task.

   The Change Logical Partition Controls window displays.

   Note: Changing logical partition control settings on a CPC can be considered disruptive. If the CPC is locked, unlock it.
2. Depending on the physical processors installed in your system (CPs, ICFs, IFLs, and zIIPs), select the processor assignment tab to display the processor assignment window. Each processor assignment window lists the logical partitions that can be activated on the CPC and displays check boxes, entry fields, and other controls that indicate their current control settings:
   - Each logical partition's settings for logical processor assignments, including the number of logical processors assigned to each logical partition, and how they are assigned as either dedicated or shared processor resources. The defined capacity weights and current weight. Workload manager (WLM) the current, minimum, and maximum processing weight.
3. Select the Processor Running Time tab.
4. Use the controls to change the control settings of the logical partitions or the CPC, then proceed to indicate what you want to do with the new settings.
5. Use the controls to change:
   - One or more logical partition's settings for how logical processors are assigned as either dedicated or shared processor resources.
   - The processing weights of logical partitions that share central processors (and whether they are capped).
   - A logical partition to be workload managed with minimum and maximum weight values to set.
   - Defined capacity values for software pricing.
   - The CPC's settings for processor running time.

Change Logical Partition Controls

Note: This task is not available when one or more managed systems have DPM enabled.

Use this window to review or change logical processor assignments of logical partitions and the system settings for processor running time:

- Displays the last rest profile attempted for the most recent activation of the system.

  Note: If the field is blank, then the system was brought to its current state and status by operations other than activation.
- Displays the identifier of the Input/output Configuration Data Set (IOCDS) used during the most recent power-on reset and the processor controls for logical partitions defined by this IOCDS.
- “Logical processor assignment tabs” on page 377 identify the number of logical processors and type of physical processors assigned to logical partitions, and set processing weights for logical partitions that share central or internal coupling facility processors (and whether they are capped).
- Settings for the “Processor Running Time tab” on page 378 control how the system manages logical partition use of the logical processors assignment.

The processor controls of the system and logical partitions are established by the activation profiles used to activate them. Ordinarily, after the system is activated, changing its processor controls requires opening and customizing a reset profile, and then using the profile to activate the system again. Likewise, when the system is activated, changing the processor controls of its logical partitions requires opening and customizing their image profiles, and then using the profiles to activate the logical partitions.

Note: Depending on your user role assignment, you may only be able to view LPAR controls.

This window allows changing some processor controls *dynamically* (new settings take effect without customizing profiles or activating objects). You can dynamically change:

- The processing weights of logical partitions that share processors (and whether they are capped).
- Allow a partition to be workload managed and set a minimum and maximum weight value.
- Allow software pricing to change based on the number of Workload Units (WLUs).
- The CPC's settings for processor running time.
- The absolute capping of logical partitions that share processors.

Additional functions on this window include:

Save to Profiles
If you want the new settings to take effect whenever the selected system and its logical partitions are activated with the modified profiles, click **Save to Profiles**. Saving new settings modifies the following activation profiles:

- A logical partition's control settings are saved in its image profiles. The settings take affect whenever the logical partition is activated with its image profile.
- The system's settings for processor running time are saved in the reset profile identified by the Last reset profile attempted filed. The settings take affect whenever the system is activated with that reset profile.

Note: Saving processor controls to activation profiles saves *all* processor controls currently displayed, regardless of when the settings were set.

Change Running System
If you change the logical partition group controls, click **Change Running System** if you want the new settings to take effect immediately. The selected system and its active logical partitions are referred to here as the *running system*. Using new settings to change the running system:

- Makes the processing weight, capped setting, and absolute capping currently displayed for each active logical partition (that shares central processors) take affect.
- Makes the settings currently displayed for system processor running time take affect.

The new settings remain in effect for the system and active logical partitions until you either dynamically change their processor controls again or activate them (which makes the processor controls in their activation profiles take affect).

Note: The running system includes active logical partitions only (as indicated by the **Active** column). Changes made to processor controls of inactive logical partitions do*not* take affect upon changing the running system. Consider saving the changes to profiles instead, to make them take affect when the logical partitions are activated.

Save and Change

If you change the logical partition group controls, click **Save and Change** if you want the new settings to take effect immediately *and* whenever the selected system and its logical partitions are activated with the modified profiles. **Save and Change** performs the combined operations of **Save to Profiles** and **Change Running System**.

Saving new settings modifies the following activation profiles:

- A logical partition's control settings are saved in its image profile. The settings take affect whenever the logical partition is activated with its image profile.
- The system's settings for group capacity value is saved in the group profile. The settings take affect immediately if any logical partitions assigned to the group are currently active or whenever any logical partition assigned to the group is activated.

Reset
To discard the information shown and display the information most recently used, click **Reset**.

Cancel
To close this window without saving changes and exit the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Logical processor assignment tabs

Depending on what physical processors are installed in your system, select the logical processor assignment tab from the window to change the settings of one or more processor controls for the logical processor assignments for:

- Logical partitions with Central Processors (CPs)
- Logical partitions with Internal Coupling Facility (ICF) processors
- Logical partitions with IBM zEnterprise® Application Assist Processor (zAAP) processors (Version 2.12.1 and earlier)
- Logical partitions with Integrated Facility for Linux (IFL) processors
- Logical partitions with z Integrated Information Processors (zIIPs)

Review the information displayed for each possible logical partition processor assignment. The table for each logical processor assignment displays processor controls for the logical partitions and processor running time. You can change the settings of one or more processor controls, then make a selection to indicate when you want the new settings to take effect.

Logical Partition
Displays the name of each logical partition defined by the IOCDS.

Active
Indicates whether each logical partition is activated.

Defined Capacity
Use this column to change the number of Workload Units (WLUs) that are assigned for each logical partition.

Note: Defined capacity can only be changed for central processors.

Workload Manager (WLM) managed
Use this column to allow the partition to be managed by Workload Manager (WLM).

Current Weight
Displays the current processing weight setting in each logical partition's logical processor assignment.

Initial Weight
Use the entry fields in this column to change the initial processing weight of logical partitions that share processors of each logical partition's logical processor assignment.

Minimum Weight
Use the entry fields in this column to change the minimum processing weights of logical partitions. When **WLM Managed** is enabled, a logical partition's minimum weights places a lower limit on the amount of shared processor resources.

Maximum Weight
Use the entry fields in this column to change the maximum processing weights of logical partitions. When **WLM Managed** is enabled, a logical partition's maximum weights places an upper limit on the amount of shared processor resources.

Current Capping
Displays the current capping setting in each logical partition's logical processor assignment.

Initial Capping
Use the entry fields in this column to change whether the processing weights of logical partitions that share central or internal coupling facility processors are capped.

“Absolute Capping” on page 381
Displays the current absolute capping setting in each logical partition's logical processor assignment. Select the current absolute capping to change the setting.

Number of Dedicated Processors
Displays the number of dedicated processors in each logical partition's logical processor assignment.

Number of Not dedicated Processors
Displays the number of non-dedicated processors in each logical partition's logical processor assignment.

Processor Running Time tab

Select the **Processor Running Time** tab to display a window allowing you to change the settings on how the selected Central Processor Complex (CPC) manages logical partition use of shared processor resources.

Processor running time is the amount of continuous time allowed for logical processors to perform jobs on shared processors. The amount of continuous time is referred to also as a *timeslice*.

Shared processors are used by all logical partitions activated without dedicated processor resources. So the processor running time, or timeslice, is assigned to all logical partitions activated without dedicated processor resources.

The processor running time can be calculated dynamically by the CPC, or set to a constant amount. The initial method for calculating the running time is set by the activation profile used to activate the CPC.

Use the settings to change the CPC's processor running time settings. Then make a selection to indicate when you want the new settings to take effect.

Note: When the window is displayed, the CPC's *current* settings for processor running time appears. Since the window allows changing the settings at any time, the CPC's current settings may not be the same as its *initial* settings. The initial settings were established by the reset profile used to activate the CPC.

You can find more detailed help on the following elements of this window:

Dynamically determined by the system

To have the CPC calculate the running time whenever the number of active logical processors changes, select **Dynamically determined by the system**.

Determined by the user

To set a constant running time, select **Determined by the user** to indicate whether logical partitions lose their share of running time when they enter a wait state.

Note: When processor running time is dynamically determined, it reduces the possibilities for suboptimal use of processor resources.

Running time

If you selected **Determined by the user** to set a constant running time, specify the constant running time you want to set.

Workload Manager (WLM) managed

Workload Manager allows the processing weights to be redistributed according to where WLM believes the CPU resources are needed to satisfy customer workload goals. This function works for uncapped shared logical processors only. The weight will be allowed to vary in a range between the minimum weight and maximum weight.

Notes:

- Only **General** mode logical partitions can be enabled for WLM management.

- Enablement of WLM managed in a logical partition is not allowed if **Initial Capping** is selected, and conversely initial capping cannot be selected if WLM managed is selected. However, it is valid for both not to be selected.
- Enablement of WLM in a logical partition and a fully dedicated logical partition are mutually exclusive.

Initial Weight

Use this field to change the initial processing weights of logical partitions that share processors.

For each logical partition that has at least one non-dedicated processor in its logical processor assignment, the field in this column displays:

- The initial processing weight assigned to each active logical partition.
- The initial weight set in the image profile of each inactive logical partition.

The processing weight can be from 1 to 999. To change a logical partition's setting, enter a new initial processing weight in its field, then use the processor controls to indicate when you want the new settings to take effect.

A logical partition's *initial processing weight* is its relative amount of shared processor resources. The exact percentage of resources allocated to the logical partition depends on the processing weights of other logical partitions defined and activated on the central processor complex (CPC) at the same time. That percentage is calculated by dividing the logical partition's processing weight by the total processing weight of all active logical partitions.

An initial processing weight is a target, not a limit. It represents the share of resources guaranteed to a logical partition when all processor resources are in use. Otherwise, when excess processor resources are available, the logical partition can use them if necessary. When a logical partition is not using its share of processor resources, other active logical partitions can use them.

While excess processor resources are available, initial processing weights have no effect on how those resources are used. Instead initial processing weights take effect only when the number of logical processors requiring a timeslice is greater than the number of available physical processors.

Notes:

- A field is available for a logical partition only when its logical processor assignment includes at least one non-dedicated processor (as indicated in the **Number of Not dedicated Processors** column. Otherwise, if its logical processor assignment includes only dedicated processors, this field is grayed-out.
- If the logical partition contains any non-dedicated processors that are reserved, they will not appear in the column **Number of Not dedicated Processors**. However, the **Initial Weight** and **Initial Capping** fields can be changed.
- An *initial* processing weight was assigned to each active logical partition by its image profile during activation. Since, the window allows changing the initial processing weight at any time, a logical partition's current setting may not be the same as its initial setting.
- The initial weight displayed for an inactive logical partition does not apply if its image profile does not exist.

Minimum Weight

Use this field to change the initial processing weights of logical partitions that share processors.

For each logical partition that has at least one non-dedicated processor in its logical processor assignment, the field in this column displays only when WLM Managed is enabled.

The minimum weight must be less than or equal to the initial processing weight.

When Workload Manager is enabled, a logical partition's *minimum weight* places a lower limit on the amount of shared processor resources. The exact percentage of resources allocated to the logical partition depends on the processing weights of other logical partitions defined and activated on the central processor complex (CPC) at the same time.

Note: A *minimum* processing weight was assigned to each active logical partition by its image profile during activation. Since the window allows changing the minimum processing weight at any time, a logical partition's current setting may not be the same as its initial setting. The initial settings were established by the reset profile used to activate the CPC.

- The minimum processing weight displayed for an inactive logical partition is not applicable if its image profile does not exist.

Maximum Weight

Use this field to change the initial processing weights of logical partitions that share processors.

For each logical partition that has at least one non-dedicated processor in its logical processor assignment, the field in this column displays only when WLM Managed is enabled.

The maximum weight must be greater than or equal to the initial weight.

When Workload Manager is enabled, a logical partition's *maximum weight* places a upper limit on the amount of shared processor resources. The exact percentage of resources allocated to the logical partition depends on the processing weights of other logical partitions defined and activated on the central processor complex (CPC) at the same time.

Note: A *maximum* weight was assigned to each active logical partition by its image profile during activation. Since the window allows changing the maximum weight at any time, a logical partition's current setting may not be the same as its initial setting. The initial settings were established by the reset profile used to activate the CPC.

- The maximum processing weight displayed for an inactive logical partition is not applicable if its image profile does not exist.

Initial Capping

Use this field to change the initial processing weights of logical partitions that share processors.

For each logical partition that has at least one non-dedicated processor in its logical processor assignment, the field in this column displays:

- Whether the initial processing weight of each active logical partition currently is capped.
- Whether the initial processing weight set in the image profile of each inactive logical partition is capped.

A check indicates the logical partition's initial processing weight is capped.

A logical partition's *initial weight* is its relative amount of shared processor resources. The *Initial Capping* setting indicates whether the logical partition is prevented from using processor resources in excess of its processing weight.

- When the initial processing weight is *not* capped, it is a target, not a limit. It represents the share of resources guaranteed to a logical partition when all processor resources are in use. Otherwise, when excess processor resources are available, the logical partition can use them if necessary.
- When the initial processing weight is capped, it is a limit. It represents the logical partition's maximum share of resources, regardless of the availability of excess processor resources.

Notes:

- A field is available for a logical partition only when its logical processor assignment includes at least one non-dedicated processor (as indicated in the **Number of Not dedicated Processors** column. Otherwise, if its logical processor assignment includes only dedicated processors, the field is grayed-out.
- If the logical partition contains any non-dedicated processors that are reserved, they will not appear in the column **Number of Not dedicated Processors**. However, the **Initial Weight** and **Initial Capping** fields can be changed.
- An *initial* capped setting was assigned to each active logical partition by its image profile during activation. Since, the window allows changing the setting at any time, a logical partition's current setting may not be the same as its initial setting.

- **Initial Capping** cannot be selected if WLM managed is already selected, as they are mutually exclusive. Conversely, WLM managed cannot be selected if initial capping is selected. However, it is valid for both not to be selected.

Absolute Capping

Use this field to change the absolute capping of logical partitions that share processors.

For each logical partition that has at least one non-dedicated processor in its logical processor assignment, the field in this column displays:

- The absolute capping assigned to each active logical partition.
- The absolute capping set in the image profile of each inactive logical partition.

The absolute capping can be None or a number of processors value from 0.01 to 255.0. To change a logical partition's setting, select the current absolute capping setting in its field, then use the Change LPAR Controls window to specify the absolute capping for the selected logical partition to indicate when you want the new settings to take effect.

While excess processor resources are available, absolute capping has no effect on how those resources are used.

Notes:

- A field is available for a logical partition only when its logical processor assignment includes at least one non-dedicated processor (as indicated in the **Number of Not dedicated Processors** column. Otherwise, if its logical processor assignment includes only dedicated processors, this field is grayed-out.
- If the logical partition contains any non-dedicated processors that are reserved, they will not appear in the column **Number of Not dedicated Processors**.
- The absolute capping displayed for an inactive logical partition does not apply if its image profile does not exist.

Edit Absolute Capping

Use this window to specify the absolute capping of the selected logical partitions that share processors.

None
To choose not to specify absolute capping, select **None**.

Number of processors (0.01 to 255.00)
To specify the number of processors, select **Number of processors (0.01 to 255.00)** and then in the input area specify a number in the range of 0.01 to 255.00 in increments of .01.

Additional functions on this window include:

OK
To save the new values and return to the previous window, click **OK**.

Cancel
To close the window without saving the changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Change LPAR Cryptographic Controls

Accessing the Change LPAR Cryptographic Controls task

The settings that determine how the activated logical partition uses the Crypto Express feature assigned to are referred here as cryptographic controls.

Logical partition's initial cryptographic controls are established by the activation profile used to activate the logical partition. See the **Customize/Delete Activation Profiles** task for more information about customizing activation profiles for establishing a logical partition's initial cryptographic controls:

You can use the Support Element workplace to start the task to select cryptographic control settings to be changed dynamically on the system, in the image profile, or both.

To dynamically change logical partition cryptographic controls:

1. Open the **Change LPAR Cryptographic Controls** task.
2. Use the Change LPAR Cryptographic Controls window to change the crypto configuration for a logical partition then proceed to indicate what you want to do with the new settings.
3. Use the cryptographic controls to dynamically:
   - Add unassigned crypto(s) domain(s) to a logical partition for the first time.
   - Edit assigned crypto(s) and domain(s) types to a logical partition already using cryptos and domains.
   - Remove crypto(s) and domain(s) from a logical partition.

Change LPAR Cryptographic Controls

Use this window to customize information that controls how the logical partition activated by the profile uses the coprocessors and accelerators assigned to it. The settings are referred to here as *cryptographic controls* and apply to the logical partition only if it is customized for using coprocessors and accelerators. This window allows you to:

- Add unassigned crypto(s) and domain(s) to a logical partition for the first time
- Edit assigned crypto(s) and domain(s) types to a logical partition already using cryptos and domains.
- Remove crypto(s) and domain(s) from a logical partition.

The assigned cryptographic domain index table displays the control domain and control and usage domain indexes which can be modified in the logical partition.

Control Domain
A logical partition's *control domains* are those cryptographic domains for which remote secure administration functions can be established and administered from this logical partition.

If you are using the Integrated Cryptographic Service Facility (ICSF), refer to ICSF documentation for information about ICSF basic operations.

If you are using a Trusted Key Entry (TKE) workstation to manage cryptographic keys, the TKE documentation provides information about selecting control domains and usage domains for a logical partition that is a TKE host or a TKE target.

Control and Usage Domain
A logical partition's *control and usage domains* are domains in the cryptos that can be used for cryptographic functions. The usage domains cannot be removed if they are online.

A logical partition's control domains can also include the usage domains of other logical partitions. Assigning multiple logical partitions' usage domains as control domains of a single logical partition allows using it to control their software setup.

If you are using the Integrated Cryptographic Service Facility (ICSF), refer to ICSF documentation for information about ICSF basic operations.

If you are using a Trusted Key Entry (TKE) workstation to manage cryptographic keys, the TKE documentation provides information about selecting control domains and usage domains for a logical partition that is a TKE host or a TKE target.

The assigned cryptos index table displays the cryptographic candidate list and cryptographic online list settings which can be modified in the logical partition.

Cryptographic Candidate List
The candidate list identifies which cryptos will be assigned to the logical partition. Cryptos cannot be removed if they are online.

Cryptographic Online List (from profile)
The online list identifies which cryptos will be brought online at the next activation. Changes to the online list do not affect the running system. You must activate the partition to bring the coprocessor or accelerators online.

You can work with the tables by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Edit
Allows you to "Edit Domains" on page 541 or "Edit Cryptos" on page 542 for the selected activation profile.

Remove
Allows you to remove selected control and usage domain settings or selected crypto candidate and online settings for the selected activation profile.

Add
Allows you to "Add Domains" on page 542 or "Add Cryptos" on page 542 for unassigned domains or unassigned crypto candidates for the selected activation profile.

The icons perform the following functions in the Assigned domains or crypto tables:

Select All
Selects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Deselect All
Deselects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header to change from ascending to descending order. Click **OK** when you have defined your preferred order.

Clear All Sorts
Returns the table back to the default order.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Save and Change

If you want the new settings to take effect immediately *and* whenever the logical partition is activated with the modified profile click "Save and Change" on page 384.

Save to Profiles
If you want the new settings to take effect whenever the logical partition is activated with the modified profile, click "Save to Profiles" on page 384.

Change Running System
If you want the new settings to take effect in the active logical partition immediately, click "Change Running System" on page 384.

Reset
To return the values back to their original values, click **Reset**.

Cancel
To close this window and exit this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Save to Profiles

Saving new settings modifies the following activation profiles:

- Saves a logical partition's cryptographic control settings in its image profile. The settings take effect whenever the logical partition is activated with its image profile.
- Saves a logical partition's cryptographic control settings for both active and inactive logical partitions. The partition status (active/inactive) is indicated in the window title, along with the logical partition name.

Change Running System

Changes the cryptographic settings in the logical partition without reactivating the partition. The new settings remain in effect for the logical partition until you either dynamically change the settings again or reactivate the partition.

Note: Change Running System can be selected for an active logical partition only. For an inactive partition, the Change Running System button will be disabled.

Save and Change

Saving new settings modifies the following activation profiles:

- Saves a logical partition's cryptographic control settings in its image profile. The settings take effect whenever the logical partition is activated with its image profile.
- Changes the cryptographic settings in the logical partition without reactivating the partition. The new settings remain in effect for the logical partition until you either dynamically change the settings again or reactivate the partition.

Note: Save and Change can be selected for an active logical partition only. For an inactive partition, the Save and Change button will be disabled.

To perform both **Save to Profiles** and **Change Running System** at the same time, click **Save and Change**. For more information about the operations, select:

- Save to Profiles
- Change Running System

Usage Domain Zeroize

When removing one or more cryptos and/or usage domains from an active logical partition, the Usage Domain Zeroize window will be displayed. This window may contain one or both of the following:

- The crypto and usage domain combinations which can zeroized.
- The crypto and usage domain combinations which already have zeroize pending.

Zeroize of the usage domain indexes will clear the cryptographic keys from the cryptographic number in the selected partition. The cryptographic keys will have to be reentered to re-enable cryptographic operations in this partition.

Click **Options** on the menu bar to *select all the rows*, *deselect all the rows*, or *exit* the window, returning to the Change LPAR Cryptographic Controls window.

Additional functions on this window include:

OK

To close this window and continue with the crypto operation, click **OK**.

Cancel

To close this window and return to the Change LPAR Crypto Controls window, click **Cancel**.

Help

To display help for the current window, click **Help**.

Usage domain zeroize and usage domain zeroize pending tables

The **usage domain zeroize** table will contain one row for each cryptographic number and usage domain combination which can zeroized. By default, all combinations are selected for zeroize. Any or all rows can be deselected so that the zeroize is not performed for those combinations.

The **usage domain zeroize pending** table will contain one row for each cryptographic number and usage domain combination that already has zeroize pending. If a zeroize is pending, these combinations cannot be selected for zeroize.

Cryptographic Number

Displays the cryptographic number which will be zeroized

Usage Domain Index

Displays the usage domain index which will be zeroized

The Usage Domain Zeroize window may contain one or both of these tables.

Change LPAR Group Controls

Accessing the Change LPAR Group Controls task

Note: This task is not available when one or more managed systems have DPM enabled.

The group assignment for logical partitions determines how allocation and management of processor resources assigned to the logical partitions in a group can be activated on the central processor complex (CPC).

You can use the Support Element workplace to start the task for reviewing or changing the group assignment for logical partitions. The group name, member partitions, and group capacity value display. A logical partition can become a member of a group which allows determining the allocation and management of processor resources assigned to logical partitions in a group. You can change a group assignment dynamically for the active logical partitions.

Note: If you add a new logical partition member to the group, a new group capacity value does not take affect if other logical partition members of the group are active. All logical partition members of the group must be deactivated first before the new group capacity value can take affect.

To review or change logical partition group controls for the selected CPC:

1. Open the **Change LPAR Group Controls** task.

   The Change Logical Partition Group Controls window displays.
2. Use the controls to change the group capacity or logical partition group members.

Change Logical Partition Group Controls

Note: This task is not available when one or more managed systems have DPM enabled.

Use this window to view or change a group assignment for logical partitions. This window displays the group name, member partitions, group capacity value, and absolute capping setting that can be customized in determining the allocation and management of processor resources assigned to the group.

Note: Depending on your user role assignment, you may only be able to view group LPAR controls.

This window allows changing a group assignment dynamically for active logical partitions.

Click **Edit** on the menu bar to select the following:

- Edit Group Capacity to change the group capacity value for a defined logical partition group.

- Edit Group Members to assign partitions to a group.
- "Edit Absolute Capping" on page 387 to change the absolute capping value for a processor type in a defined logical partition group.

The table list the group assignments for the logical partitions that can be customized:

Group Name
Displays the group name for the logical partition(s)

Member Partitions
Displays the name(s) of the logical partitions assigned to the group

Group Capacity Value
Displays the number of Workload Units (WLU) that are assigned to the logical partitions group.

Absolute Capping
Displays the current absolute capping setting for each logical partition's logical processor assigned to the group.

Additional functions on this window include:

Save to Profiles
If you want the new settings to take effect whenever the selected system and its logical partitions are activated with the modified profiles, click **Save to Profiles**.

A logical partition's group name is saved in the image profile and the group capacity value is saved in the group profile. The settings take effect whenever any logical partition assigned to the group is activated with its image profile.

Note: Saving processor controls to activation profiles saves *all* processor controls currently displayed, regardless of when the settings were set.

Change Running system
If you change the logical partition group controls, click **Change Running System** if you want the new settings to take effect immediately. The selected system and its active logical partitions are referred to here as the *running system*. Using new settings to change the running system makes the new group name and group capacity setting currently displayed for each active logical partition (that shares central processors) take effect.

The new settings remain in effect for the system and active logical partitions until you either dynamically change their processor controls again or activate them (which makes the processor controls in their activation profiles take effect).

Note: The running system includes active logical partitions only (as indicated by the **Partition Active** column). A group becomes part of the running system when any member partition assigned to the group is activated. The group capacity value can be changed for the running system as long as the group has one active partition. Changes made to group controls of inactive logical partitions do *not* take effect upon changing the running system. Consider saving the changes to profiles instead, to make them take effect when the logical partitions are activated.

Save and Change

If you change the logical partition group controls, click **Save and Change** if you want the new settings to take effect immediately *and* whenever the selected Central Processor Complex (CPC) and its logical partitions are activated with the modified profiles. **Save and Change** performs the combined operations of **Save to Profiles** and **Change Running System**.

Saving new settings modifies the following activation profiles:

- A logical partition's group name is saved in its image profile. The settings take effect whenever the logical partition is activated with its image profile.
- The group capacity value is saved in the group profile. The settings take effect immediately if any logical partitions assigned to the group are currently active or whenever any logical partition assigned to the group is activated.

Reset
To discard the information shown and display the information most recently used, click **Reset**.

Cancel
To close this window without saving changes and exit the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Edit Group Capacity

Use this window to specify a group capacity value for all logical partitions belonging to this group.

Additional functions on this window include:

OK
To apply the group capacity value and return to the previous window, click **OK**.

Cancel
To close the window without saving changes and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Edit Group Members

Use this window to assign logical partition(s) to a group or to remove logical partition(s) from a group.

Partition Name
Displays the name of the partition

Partition Active
Indicates whether the partition is active

Current Group
Displays the current name of the group

New Group
Enter the name of the new group to which the partition(s) will be assigned or enter "NONE" to remove a partition from a group

You can find more detailed help on the following elements of this window:

OK
To apply the new changes to a group and return to the previous window after assigning partitions to a group, click **OK**.

Cancel
To close the window without saving changes and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Edit Absolute Capping

Use this field to change the absolute capping of logical partitions in a group that share processors. The absolute capping can be None or a number of processors value from 0.01 to 255.0. To change an absolute capping for a processor type for a group, select the current absolute capping setting in its field and click the hyperlink to display the next Edit Absolute Capping window. Specify the absolute capping for the selected processor type to indicate the new setting.

Additional functions on this window include:

OK
To save the new values and return to the previous window, click **OK**.

Cancel
To close the window without saving the changes window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Refer to the following for additional information on the Edit Absolute Capping table functions:

Edit Absolute Capping

Use this window to specify the absolute capping of the selected processor type belonging to this group.

None
To choose not to specify absolute capping, select **None**.

Number of processors (0.01 to 255.00)
To specify the number of processors, select **Number of processors (0.01 to 255.00)** and then in the input area specify a number in the range of 0.01 to 255.00 in increments of .01.

OK
To save the new values and return to the Change LPAR Group Controls window, click **OK**.

Cancel
To close the window without saving the changes you made and return to the Change LPAR Group Controls window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Change LPAR I/O Priority Queuing

Accessing the Change LPAR I/O Priority Queuing task

This task allows you to review or change the minimum or maximum input/output (I/O) priority queuing value assignments of logical partitions. These values are passed on to the I/O subsystem for use when queuing decisions with multiple requests. You can dynamically (new settings take effect without customizing profiles or activating objects) change the minimum and maximum input/output (I/O) priority queuing values. See setting the I/O priority queuing values to customize the activation profile for each logical partition.

To change LPAR I/O priority queuing:

1. Open the **Change LPAR I/O Priority Queuing** task.

   The Change Logical Partition Input/Output (I/O) Priority Queuing window displays. The window lists the I/O priority queuing values for logical partitions defined by this IOCDS.

2. Use the window to dynamically change the minimum and maximum I/O priority queuing values.

   Note: If global input/output I/O priority queuing is **Enabled**, changes made for the minimum or maximum values will take effect immediately. If the global value is **Disabled**, changes will be saved by the system, but will not take effect until the global value is changed to **Enabled**.

3. Make a selection to indicate what you want to do with the new setting.

Change Logical Partition Input/Output (I/O) Priority Queuing

Use this window to review or change the minimum and maximum Input/Output (I/O) priority queuing values of logical partitions *dynamically*. (New settings take effect without customizing profiles or activating objects.)

The I/O priority queuing values of the logical partitions are established by the activation profiles used to activate them. Ordinarily, after a CPC is activated in LPAR mode, changing the I/O priority queuing values of its logical partitions requires opening and customizing its image profiles and then using the profiles to activate the logical partitions.

A range of priorities for a logical partition are supported. These values are passed to the I/O subsystem for use when making queuing decisions with multiple requests.

1. Review the information displayed in the window's fields.

2. You can change the settings of one or more priority queuing values by typing values into the table:
   - *Minimum input/output (I/O) priority queuing values* specify a minimum priority to associate with an Input/Output (I/O) request at Start Subchannel time for the logical partition.
   - *Maximum input/output (I/O) priority queuing values* specify a maximum priority to associate with an Input/Output (I/O) request at Start Subchannel time for the logical partition.
3. To indicate when you want the new settings to take effect, click **Save to Profiles**, **Change Running System**, or **Save and Change**.

The following functions are available from this window:

Input/output configuration data set (IOCDS)
Displays the identifier of the IOCDS used during the most recent power on.

Global input/output (I/O) priority queuing
Indicates whether the global input/output (I/O) priority queuing is enabled or disabled.

Note: If global input/output (I/O) priority queuing is enabled, changes made for the minimum or maximum values take effect immediately. If the global value is disabled, changes are saved by the system, but do not take effect until the global value is changed to enabled.

Maximum global input/output (I/O) priority queuing value
Indicates the maximum value allowed in the current system for Input/Output (I/O) priority queuing. This is the highest value to which any of the partition's minimum or maximum Input/Output (I/O) priority queuing value can be set. Changes made on the panel are passed to the I/O subsystem if I/O priority queuing is enabled for use when making queuing decisions with multiple requests.

Note: The Input/Output (I/O) priority queuing values for the partition can be equal to or less than the global maximum Input/Output (I/O) priority queuing value, ensuring that the rules stated for minimum and maximum are met as well.

Logical partition table

This table lists the following information:

Logical Partition
This column displays the name of each logical partition defined by the IOCDS.

Active
This column indicates whether each logical partition is activated.

A logical partition becomes *active* when it is activated. Conversely, a logical partition is not active, or is *inactive*, before it is activated and after it is deactivated.

- **Yes** - Indicates the logical partition currently is activated.

  Note: An active logical partition is not necessarily operating.
- **No** - Indicates the logical partition currently is not activated.

Minimum Input/Output (I/O) Priority
Use this column to change the minimum priority associated with an Input/Output (I/O) request at Start Subchannel time for the logical partition. This minimum value is passed to the I/O subsystem if I/O priority queuing is enabled for use when making queuing decisions with multiple requests.

Note:

- The minimum value must be less than or equal to the maximum value.
- The minimum value must be less than or equal to the **maximum global Input/Output (I/O) priority queuing value**.
- The I/O priority values can overlap with the I/O priority values for other active logical partitions.
- The minimum value also serves as the default I/O priority value for the logical partition. If the software in the logical partition does not understand I/O priority queuing, the minimum value is assigned to all I/O requests in the logical partition. In this case, for clarity, the maximum value should be set equal to the minimum value, although this is not a requirement.

- The logical partition default value for the minimum priority is zero.
- Setting both the minimum and maximum values to zero for a logical partition has a disabling effect on I/O priority queuing for that logical partition. Use caution in doing this because the logical partition would then have the lowest priority possible.

Maximum Input/Output (I/O) Priority
Use this column to change the maximum priority associated with an Input/Output (I/O) request at Start Subchannel time for the logical partition. This maximum value is passed to the I/O subsystem if I/O priority queuing is enabled for use when making queuing decisions with multiple requests.

Note:

- The maximum value must be greater than or equal to the minimum value.
- The maximum value must be less than or equal to the **maximum global Input/Output (I/O) priority queuing value**.
- The I/O priority values can overlap with the I/O priority values for other active logical partitions.
- The logical partition default value for the maximum priority is zero.
- Setting both the minimum and maximum values to zero for a logical partition has a disabling effect on I/O priority queuing for that logical partition. Use caution in doing this because the logical partition would then have the lowest priority possible.

Save to Profiles
If you change the settings of one or more priority queuing values and you want the new settings to take effect whenever the Central Processor Complex (CPC) and logical partitions are activated with the modified profiles, click **Save to Profiles**.

Saving new settings changes the image profile. A logical partition's minimum and maximum Input/Output (I/O) priority queuing settings are saved in its image profile. The settings take effect whenever the logical partition is activated with its image profile.

Note: Be aware that saving priority queuing values to activation profiles saves *all* priority queuing values currently displayed, regardless of when the settings were set. For example, if you used the **Change Logical Partition Input/Output (I/O) Priority Queuing** window previously to change some of the running system's I/O priority queuing settings, those changes are saved in the profiles along with any changes you made presently.

Change Running System
If you change the settings of one or more priority queuing values and you want the new settings to take effect immediately, click **Change Running System**.

The Central Processor Complex (CPC) and its active logical partitions are referred to here as the *running system*. Using new settings to change the running system makes the minimum and maximum Input/Output (I/O) priority queuing setting currently displayed for each active logical partition (that shares central processors) take effect.

The new settings remain in effect for the CPC and active logical partitions until you either dynamically change their priority queuing values again or activate them (which makes the priority queuing values in their activation profiles take effect).

Note: The running system includes active logical partitions only (as indicated by the **Active** list column). Changes made to priority queuing values of inactive logical partitions do *not* take effect upon changing the running system. Instead, consider saving the changes to profiles to make them take effect when the logical partitions are activated.

Reset
To discard changes you made to the settings of priority queuing values and display again the current settings, click **Reset**.

Cancel
To close this window without saving the changes you made and exit the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Change LPAR Security

Accessing the Change LPAR Security task

The settings that determine the extent of interaction between logical partitions that can be activated on the central processor complex (CPC) are referred to here as *security settings*.

A logical partition's security settings are:

Performance data control
This setting controls whether a logical partition has global access to performance data.

Input/output configuration control
This setting controls whether a logical partition can change the input/output (I/O) configuration of the CPC on which it is activated.

Cross partition authority
This setting controls whether a logical partition can issue a subset of control program instructions to other logical partitions activated on the same CPC

Logical partition isolation
This setting controls whether a logical partition has exclusive use of its reconfigurable channel paths.

Basic counter set authorization control
The basic set authorization control can be used in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is running.

Problem state counter set authorization control
The problem state set authorization control can be used in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is in problem state.

Crypto activity counter set authorization control
The crypto activity counter set authorization control can be used to identify the crypto activities contributed by the logical CPU and the blocking effects on the logical CPU.

Extended counter set authorization control
The counters of the extended counter set authorization control are model dependent.

Basic sampling authorization control
The basic sampling authorization control allows tooling programs to map instruction addresses into modules or tasks, and facilitates determination of hot spots.

Dynamic sampling authorization control
The dynamic sampling authorization control allows tooling programs to map instruction addresses into modules or tasks, and facilitates determination of hot spots.

Permit AES key import functions
The permit Advanced Encryption Standard (AES) key import functions allow you to enable the new Perform Cryptographic Key Management Operation functions of the CP Assist for Cryptographic Functions (CPACF) feature.

Permit DEA key import functions
The permit Data Encryption Algorithm (DEA) key import functions allow you to enable the new Perform Cryptographic Key Management Operation functions of the CP Assist for Cryptographic Functions (CPACF) feature.

Permit ECC key import functions
The permit Elliptical Curve Cryptography (ECC) key import functions allow you to enable the new Perform Cryptographic Key Management Operation functions of the CP Assist for Cryptographic Functions (CPACF) feature.

A logical partition's initial security settings are established by the activation profile used to activate the logical partition. See the **Customize/Activation Profiles** task for more information about customizing activation profiles for establishing a logical partition's initial security settings:

To review or change logical partition security settings:

1. Open the **Change LPAR Security** task.

   The Change Logical Partition Security window displays. The window lists the logical partitions that can be activated on the CPC and displays check boxes that indicate their current security settings:

   - Performance data control
   - Input/output configuration control
   - Cross partition security
   - Logical partition isolation
   - Basic counter set authorization control
   - Problem state counter set authorization control
   - Crypto activity counter set authorization control
   - Extended counter set authorization control
   - Basic sampling authorization control
   - Dynamic sampling authorization control
   - Permit AES key import functions
   - Permit DEA key import functions.
2. Use the check boxes to change the logical partitions' security settings, then use the controls to indicate what you want to do with the new settings.

   Use the online Help for more information about changing logical partition security.

   Notes:

   - *Dynamic I/O configuration*: Although more than one logical partition can run an application that supports dynamic I/O configuration, you should allow using only one logical partition to dynamically change the I/O configuration. The I/O configuration control setting of the logical partition you choose must display a check mark. The I/O configuration control setting of all other logical partitions should be blank.
   - *Automatic reconfiguration facility (ARF)*: To use a logical partition for running an application that supports the ARF, its cross partition authority setting must display a check mark.

Change Logical Partition Security

Use this window to review or change the security settings of logical partitions *without* opening their image profiles or activating them. The settings determine the extent of interaction between logical partitions that can be activated on the Central Processor Complex (CPC). The settings are referred to here as *security settings*.

A logical partition's operational capabilities and characteristics, which include its security settings, are established by the activation profile used to activate it. Ordinarily, after the CPC is activated in Logically Partitioned (LPAR) mode, changing the operational capabilities and characteristics of its logical partitions requires opening and customizing their image profiles, and then using the profiles to activate the logical partitions.

The window lists the security settings for logical partitions defined by the Input/Output Configuration Data Set (IOCDS) used during the most recent power-on reset of the CPC.

Reset
To discard changes you made to any security settings, and display the initial security settings for each logical partition, click **Reset**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following element of this window:

Input/Output Configuration Data Set (IOCDS)

Displays the identifier of the IOCDS used during the most recent power-on reset.

Change Logical Partition Security List

Use this window to customize security options for the activated logical partitions.

Logical Partition
Displays the name of each logical partition defined by the IOCDS.

Active
Indicates whether each logical partition is activated.

Performance Data Control
Use each check box in this list column to control whether a logical partition has global access to performance data.

Input/Output Configuration Control
Use each check box in this list column to control whether a logical partition can change the Input/Output (I/O) configuration of the CPC on which it is activated.

This control allows the OSA Support Facility to control OSA configuration for other LPs and allows access to certain STP data.

Cross Partition Authority
Use each check box in this list column to control whether a logical partition can issue a subset of control program instructions to other logical partitions activated on the same CPC.

BCPii Permissions
Select the hyperlink to change the BCPii command permissions for the running system, selected logical partitions, or both.

Logical Partition Isolation
Use each check box in this list column to control whether a logical partition has exclusive use of its reconfigurable channel paths.

Basic Counter
Use the check box in this list column to control whether authorization is allowed to use the basic counter set. The set can be used in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is running.

Problem State Counter
Use the check box in this list column to control whether authorization is allowed to use the problem-state counter set. The set can be used in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is in problem state.

Crypto Activity Counter
Use the check box in this list column to control whether authorization is allowed to use the crypto-activity counter set. The set can be used to identify the crypto activities contributed by the logical CPU and the blocking effects on the logical CPU.

Extended Counter
Use the check box in this list column to control whether authorization is allowed to use the extended counter set. The counters of this set are model dependent. This set can be used to count the crypto activities of a coprocessor.

Basic Sampling
Use the check box in this list column to control whether authorization is allowed to use the basic-sampling function which provides a set of architected sample data. The sample data includes an instruction address, the primary ASN, and some state information about the CPU. This allows tooling programs to map instruction addresses into modules or tasks, and facilitates determination of hot spots.

Diagnostic Sampling
Use the check box in this list column to control whether authorization is allowed to use the diagnostic-sampling function which provides a set of architected sample data. The sample data includes an instruction address, the primary ASN, and some state information about the CPU. This allows tooling programs to map instruction addresses into modules or tasks, and facilitates determination of hot spots.

AES Key
Use the check box in this list column to enable or disable the Advanced Encryption Standard (AES) key import functions for the installed CP Assist for Cryptographic Functions (CPACF) feature.

DEA Key
Use the check box in this list column to enable or disable the Data Encryption Algorithm (DEA) key import functions for the installed CP Assist for Cryptographic Functions (CPACF) feature.

ECC Key
Use the check box in this list column to enable or disable the Elliptical Curve Cryptography (ECC) key import functions for the installed CP Assist for Cryptographic Functions (CPACF) feature.

Note: When the window displays, the check boxes for each logical partition indicate its *current* security settings. Since the window allows changing the security settings at any time, a logical partition's current settings may not be the same as its *initial* settings. The initial settings were established by the activation profile used to activate the logical partition.

Add partition

Use this window to specify the partitions from which the target partition can receive BCPii commands.

Enter system and partition manually
System: Enter the system name for the logical partition from which the target partition can receive BCPii commands.

Netid: Enter the Netid name for the selected system.

Partition: Enter the logical partition name from which the target partition can receive BCPii commands.

Select a system and partition
System: Select from the drop-down menu the system for the logical partition from which the target partition can receive BCPii commands.

Netid: The Netid displays for the selected system.

Partition: Select from the drop-down menu the active logical partition from which the target partition can receive BCPii commands.

Additional functions on this window include:

Add
To add the system and partition, click **Add**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Configure BCPii Permissions

Use this section to enable or disable the Base Control Program internal interface (BCPii) permissions for the selected logical partition.

Enable the partition to send commands
To enable the selected partition to send BCPii commands, select **Enable the partition to send commands**. When selected, the active logical partition can send BCPii commands to other active logical partitions.

Enable the partition to receive commands from other partitions
To enable the selected partition to receive BCPii commands from other partitions, select **Enable the partition to receive commands from other partitions**. When selected, the active logical partition can receive BCPii commands from other active logical partitions.

All partitions
Select this option if you want the selected logical partition to receive BCPii commands from all the active logical partitions.

"Add partition" on page 394 (Selected partitions)
Select this option if you want to remove or add selected logical partitions to receive BCPii commands from the logical partition.

Add
To add a system and logical partition to receive BCPii commands from the logical partition, click **Add**.

Remove
To remove a selected logical partition to receive BCPii commands from the logical partition, click **Remove**.

Additional functions on this window include:

OK
To return to the previous window with updated changes, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Save and Change

If you change the security settings for the activated logical partitions, click **Save and Change** if you want the new settings to take effect immediately *and* whenever the selected Central Processor Complex (CPC) and its logical partitions are activated with the modified profiles.

Note: Saving new settings modifies the following activation profiles:

- A logical partition's security settings are saved in its image profile. The settings take effect whenever the logical partition is activated with its image profile.

Clicking **Save and Change** performs at once the two operations performed by selecting **Save to Profiles** and **Change Running System**. For more information about the operations, select:

- Save to Profiles
- Change Running System

Change Running System

If you change the security settings for the activated logical partitions, click **Change Running System** if you want the new settings to take effect immediately.

The selected Central Processor Complex (CPC) and its active logical partitions are referred to here as the *running system*. Using new settings to change the running system make the security settings currently displayed for CPC's processor running time take effect.

The new settings remain in effect for the CPC and active logical partitions until you either dynamically change their security settings again or activate them (which makes the security settings in their activation profiles take effect).

Note: The running system includes active logical partitions only (as indicated by the **Active** column). Changes made to security settings of inactive logical partitions do *not* take effect upon changing the running system. Consider saving the changes to profiles instead, to make them take effect when the logical partitions are activated.

Save to Profiles

If you change the security settings for the activated logical partitions, click **Save to Profiles** if you want the new settings to take effect whenever the selected Central Processor Complex (CPC) and its logical partitions are activated with the modified profiles.

Saving new settings modifies the following activation profiles:

- A logical partition's security settings are saved in its image profile. The settings take effect whenever the logical partition is activated with its image profile.

Note: Saving security settings to activation profiles saves *all* security settings currently displayed, regardless of when the settings were set. For example, if you used the Change Logical Partition Security window previously to change some of the running system's security settings, those changes are saved in the profiles along with any changes you made presently.

Configure BCPii Permissions

Use this section to enable or disable the Base Control Program internal interface (BCPii) permissions for the selected logical partition.

Enable the partition to send commands
To enable the selected partition to send BCPii commands, select **Enable the partition to send commands**. When selected, the active logical partition can send BCPii commands to other active logical partitions.

Enable the partition to receive commands from other partitions
To enable the selected partition to receive BCPii commands from other partitions, select **Enable the partition to receive commands from other partitions**. When selected, the active logical partition can receive BCPii commands from other active logical partitions.

All partitions
Select this option if you want the selected logical partition to receive BCPii commands from all the active logical partitions.

“Add partition” on page 394 (Selected partitions)
Select this option if you want to remove or add selected logical partitions to receive BCPii commands from the logical partition.

Add
To add a system and logical partition to receive BCPii commands from the logical partition, click **Add**.

Remove
To remove a selected logical partition to receive BCPii commands from the logical partition, click **Remove**.

Additional functions on this window include:

OK
To return to the previous window with updated changes, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add partition

Use this window to specify the partitions from which the target partition can receive BCPii commands.

Enter system and partition manually
System: Enter the system name for the logical partition from which the target partition can receive BCPii commands.

Netid: Enter the Netid name for the selected system.

Partition: Enter the logical partition name from which the target partition can receive BCPii commands.

Select a system and partition
System: Select from the drop-down menu the system for the logical partition from which the target partition can receive BCPii commands.

Netid: The Netid displays for the selected system.

Partition: Select from the drop-down menu the active logical partition from which the target partition can receive BCPii commands.

Additional functions on this window include:

Add
To add the system and partition, click **Add**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Change Mirror Time

Accessing the Change Mirror Time task

This task allows you to set up a time to daily mirror the primary Support Element to the alternate Support Element.

To schedule mirroring:

1. Select a system.
2. From the Operational Customization task list, open the **Change Mirror Time** task. The Change Mirror Time window is displayed.
3. Enter the time of day you want to schedule the daily mirroring to occur, then click **Save** to proceed or **Cancel** to close the window without setting a time.

Change Mirror Time

Use this task to update the time to mirror the Primary Support Element hard disk data to the Alternate Support Element. Ordinarily, the Support Element data is mirrored automatically each day. But you can use this task to schedule a time to mirror Support Element hard disk data to the Alternate Support Element.

Time
Provide the time of day you want to daily mirror the Support Element hard disk data to the Alternate Support Element.

Save
To save the time you provided, click **Save**.

Cancel
To exit the task without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Change Password

Accessing the Change Password task

This task allows you to change your password.

The security of information assets is controlled by user identification with passwords. Access to security functions or sensitive data is restricted by user roles.

Each user is given access to the system through a user identification and password. This password should be kept confidential and changed if necessary to maintain security.

To change your password:

1. Open the **Change Password** task. The Change Password window is displayed.
2. Enter your current password and your new password twice, the second time to confirm it.
3. Click **DONE** to change your password.

Change Password

Use this task to change your password when logging on the console.

A password verifies your user identification (user ID) and your authority to log on the console.

Complete the entry fields, then click **DONE** to change your password and then log on to the console.

Current password
Specify your current password.

New password
Specify a new password for logging on the console.

Confirm new password
Specify the new password again to verify its spelling in this field.

Note: The new password is not displayed as you type it; black dots are displayed instead.

DONE
To change your password to log onto the console, click **DONE**.

CANCEL
To close the window, and return to the window from which you selected the task, click **CANCEL**.

Channel Details

Channel Details

This window displays the current instance information and acceptable status settings for a selected channel path identifier (CHPID) of an image or the physical channel identifier (PCHID) for a selected channel of the CPC.

- **Instance Information** includes the current status of the channel path, and other information about the channel path's operating conditions and characteristics.
- **Acceptable Status** settings determine which of the channel path statuses are acceptable and which statuses are unacceptable. The Support Element console reports when the channel path status becomes unacceptable.

  Review the settings under “Acceptable Status” on page 400. Optionally, use its check boxes and click **Apply** to change the acceptable status settings.

Apply
To apply changes you made to the channel path's acceptable status settings, click **Apply**.

Advanced Facilities
To open the Advanced Facilities window for the selected channel or channel path, click **Advanced Facilities...**.

Channel Problem Determination
To open the Channel Problem Determination window for the selected channel, click **Channel Problem Determination...**.

Cancel
To close the window without saving changes you made to the channel path's acceptable status settings, click **Cancel**.

Help
To display help for the current window, click **Help**.

Instance Information

This window displays the current instance information for the selected channel path identifier (CHPID) of an image or the physical channel identifier (PCHID) for the selected channel of the CPC.

Instance Information includes the current status of the channel path, and other information about the channel path's operating conditions and characteristics.

Status
Displays the current status of the channel path.

Type
Displays one of the following:

- The channel type of the CHPID (displays for a selected CHPID of an image).
- The hardware type of the PCHID (displays for a selected channel of the CPC).
- The Crypto Express2 type (displays Accelerator or Coprocessor).

Crypto
Displays the crypto number assigned to the physical crypto adapter.

CSS.CHPID
Displays all the CSS.CHPIDs associated with that physical channel identifier (PCHID). A CSS identifies which channel subsystems the CHPID belongs to.

FID
Displays the function identifier (FIDs) for the selected channel.

CHPID Characteristics
Displays how the CHPID is defined in the IOCDS; shared, dedicated, or reconfigurable.

Adapter ID
Displays the adapter identification for the selected PCHID.

Port number
Displays the adapter port number for the selected PCHID.

Location
Displays the location number of the cage and card slot in which the channel path's channel hardware is installed. Displays the position number on the card in the slot of the channel path's jack.

Owning Image
If the central processor complex (CPC) is activated, this field indicates whether the channel path is configured to a single image or shared by multiple images.

All Owning Images
Displays one of the following:

- A list of all configured images associated with that CSS.CHPID (selected CHPID of an image).
- A list of all configured images that contain a CSS.CHPID associated with that physical channel identifier (PCHID) (selected channel of the CPC).

Network IDs
Identifies the physical layer 2 LAN fabric or physical broadcast domain. You can use this value to logically associate the system features, adapters, and ports to be physically connected to your network.

Swapped with
Displays the name of the PCHID that it is swapped with. If the PCHID is not swapped, this field displays none.

Acceptable Status

This window displays the current acceptable status settings for the channel path with the selected channel path identifier (CHPID) or the selected physical channel identifier (PCHID). *Acceptable status settings* determine which of the channel path statuses are acceptable and which statuses are unacceptable. Use the check boxes to change the settings:

- A check mark in a check box indicates an acceptable status.
- Otherwise, an empty check box indicates an unacceptable status.
- To change one setting to the other, click once on the check box.

The Support Element console continuously monitors the statuses of the channel path and compares them to the channel path's acceptable status settings.

While the statuses are acceptable, the background of the CHPID icon or PCHID icon has no color. An *exception* occurs when a status becomes unacceptable. The console reports an exception to the console operator by changing the background color of the CHPID or PCHID to the color set for indicating its specific unacceptable status. The color displayed to the right of each status in the group box is the color currently used for the background color of the CHPID or PCHID when the status is the cause of an exception. That is, the color set for a status is displayed only when the status is unacceptable and it is the current status of the channel path.

Note: To change the color set for a status, open **Support Element Settings**.

So setting the channel path's acceptable status settings allows you to control which statuses are reported as exceptions:

- Acceptable statuses, indicated by check marks in their check boxes, are not reported as exceptions.
- Unacceptable statuses, indicated by empty check boxes, are reported as exceptions.

Check stopped
The channel path is unavailable due to a permanent machine error affecting the channel hardware. The channel path is not operating.

Definition error
The channel path specified in the active input/output configuration data set (IOCDS) does not match the characteristics of the installed channel, or the channel type is incompatible with the current storage allocation, or the level of the installed channel hardware does not support the definition in the IOCD. The channel path is not operating.

Initializing
The firmware is being loaded into the channel card and then the channel card is starting.

Loss of signal
The channel path detected a link-signal error. The level of the signal on the link is below the value specified for reliable communication.

Loss of synchronization
The channel path detected a link-signal error. The bit synchronization with the signal was lost. The channel path is not operating

Not Defined
The channel path is not defined in the active IOCDS. The channel path is not operating.

No operational link
The channel path detected a link failure due to a not-operational sequence. The channel path is not operating.

No Power
The power is off for the hardware that supports the channel path. The channel path is not operating.

Operating
The channel path is operating.

Permanent error
The channel path is unavailable due to a permanent outboard error. The channel path is not operating.

Service
The channel path is in single channel service (SCS) mode and is not in the active I/O configuration. The channel path is not operating.

Suspended
The channel path is suspended. The channel path is not operating.

Wrap block
A wrap block is installed on the channel path's channel interface.

Note: Wrap blocks are used during special diagnostic tests performed on the channel. Wrap blocks must be removed prior to system initialization to allow the channel to initialize completely. The channel path is not operating.

Sequence time-out
The channel path detected a link failure due to a sequence time out. The channel path is not operating.

Sequence not permitted
The channel path detected a link failure due to an illegal sequence for a link. The channel path is not operating.

Terminal condition
The channel path is not available due to an interface-hung condition. This can occur after an interface or channel error if the control unit or device fails to disconnect from the interface when requested by the channel. The channel path is not operating

Offline signal received
The channel path detected an offline sequence, indicating that the sender is in offline mode and subsequent link-signal errors detected by the channel path are not to be reported. For an ES conversion channel, this condition can occur only when the channel is wrongly attached to another channel, switch, or control unit instead of an ESCON Converter. The channel path is not operating.

Test mode
The channel path is in test mode. The channel path is not operating

Bit error threshold exceeded
The number of bit errors the channel path detected while receiving or sending data is more than the threshold set for its bit error counter. The channel path is not operating

IFCC threshold exceeded
The number of interface control checks (IFCCs) the channel path detected is more than the threshold set for its IFCC counter. IFCCs may continue to occur, but their error logs will not be created and sent to the Support Element.

Stopped
The channel path is not operating.

I/O suppressed
The channel path has input/output (I/O) suppression active. I/O suppression prevents the channel subsystem from selecting any device and fetching the first channel command word (CCW) of a channel program. The channel path is not operating.

Fabric login sequence failure
This condition means that the channel detected a failure during that fabric login procedure

Port login sequence failure
This condition means that the channel detected a failure during the registration procedure. In order for a FICON channel to communicate with devices on a control unit, it must perform a Port Login with that control unit.

State change registration failure
This condition means that the channel detected a failure during the registration procedure. A FICON channel is required to register with the switch to receive state change notification

Invalid attachment failure
Occurs when the channel determines that it is connected to a switch, but the IOCDS specifies that is should be directly connected to a control unit or the contrary.

Save as default
To allow you to change the acceptable status for all of the current objects defined with the same status type, select **Save as default**. After you click **Apply**, a message window appears confirming that you want to proceed with this operation.

Background color of the CPC

While the statuses of the central processor complex (CPC), central processors (CPs), and channels are acceptable, the background of the CPC icon has no color. An *exception* occurs when a status becomes unacceptable. The console reports an exception to the console operator by changing the background color of the CPC to the color set for indicating its specific unacceptable status.

The background color of the CPC indicates unacceptable statuses as follows:

- Until CPC power is turned on and a power-on reset is performed, the background color of the CPC indicates an unacceptable CPC status.
- After CPC power is turned on and a power-on reset is performed:
  - The background color of the left side of the CPC indicates an unacceptable CP status.
  - The background color of the right side of the CPC indicates an unacceptable channel status.

Channel PCHID Assignment

Accessing the Channel to PCHID Assignment task

This task allows you to display the physical locations of all the installed and configured physical channels and the assigned physical channel identifier (PCHID) mapping. The CSS.CHPID associated with the PCHID and a description of the channel hardware type are displayed. The CSS.CHPID identifies the channel subsystem that the CHPID belongs to. You can view the front and back details of a specific cage. An action to write the view to a USB flash memory drive allows you to print the cage view.

To view the channel to PCHID assignments:

1. The central processor complex (CPC) must be power-on reset.
2. Locate the **CPC** to work with.
3. Open the **Channel to PCHID assignment** task.

   Channel to PCHID assignment window displays.
4. Click **View** from the menu bar to display the following menu options:
   - Sort by Channel Location
   - Sort by Cage and PCHID Number
   - Sort by Card Type and PCHID Number
   - Sort by Book and Jack and Fanout
   - Sort by Channel State
   - Sort by PCHID Number
   - Sort by Configured CSS.CHPIDs
   - View Cage Details.
5. Click **Search** from the menu bar to display the following menu options:
   - Search by PCHID
   - Search by Configured CSS.CHPID.
6. Click Exit from the **Options** menu bar to exit this window.

Channel to PCHID Assignment

Use the **Channel PCHID Assignment** task to view information that defines the channel location by cage/slot/jack to a physical channel identifier (PCHID). You can sort the view actions by channel location,

channel state, or PCHID number. You can also search for a specific PCHID number assignment or configured CSS.CHPID you want to locate.

The CSS.CHPID is a single-digit number that identifies the channel subsystem followed by a decimal point followed by a two-digit number that identifies the channel path. The CSS.CHPID(s) assigned to a PCHID in the IOCDS are displayed if a power-on reset is complete.

You can also view front and back details of a specific cage and an action to write the view to a USB Flash Memory Drive.

To display help for the current window, select **Help** from the menu bar.

The following menu bar choices are available on the **Channel to PCHID Assignment** window. You can find more detailed help on the following elements of this window:

Channel location to PCHID assignment

The Channel location to PCHID assignment displays information that defines the channel location.

Channel Location Cage/Card Slot/Jack
Displays the location number of the cage and card slot in which the channel path's channel hardware is installed. Displays the position number on the card in the slot of the channel path's jack.

Book-Fanout-jack
Displays the number of the book that is connected to the channel card, the fanout, and the jack number on the book that the STI is connected to.

Channel State
Displays the current state of the channel; standby, online, reserved, etc. The CPC must be power-on reset for this state to display.

Physical Channel ID (PCHID)
Displays the physical channel identifier (PCHID) assigned to the cage/slot/jack.

CSS.CHPID
Displays the configured CSS.CHPIDs assigned to a PCHID. The CSS.CHPID is a single-digit number followed by a decimal point followed by a two-digit number. Use the left and right scroll bar to locate all CSS.CHPIDs associated with a PCHID number.

Card Type
Displays the card type for the current channel.

View

To display information for the channel PCHID assignments, select **View** from the menu bar. You can sort information from the view actions by channel location, channel state, or by the physical channel identifier (PCHID) number.

Select an action from the list to get additional help.

Sort by Channel Location
Displays the channel to PCHID assignment sorted by cage, card slot, and jack.

Sort by Cage and PCHID Number
Displays the channel to PCHID assignment sorted by cage and then the current PCHID number assignment in ascending order.

Sort by Card Type and PCHID Number
Displays the channel to PCHID assignment sorted by card type and then the current PCHID number assignment in ascending order.

Sort by Book and Jack and Fanout
Displays the book number, the jack number on the book, and the Memory Bus Adaptor (MBA) number.

Sort by Channel State
Displays the channel state if the CPC is power-on reset; standby, online, reserved, etc.

Sort by PCHID Number
Displays the channel to PCHID assignment sorted by PCHID number.

Sort by Configured CSS.CHPIDs
Displays the channel to PCHID assignment sorted by the configured CSS.CHPID number.

View Cage Details
Displays the image of both front and back of the cage and the PCHID values in each card slot.

View Cage Details

Use **View Cage Details** to view the front and back of a specific cage. The cage view identifies the PCHID assignments and the configured CSS.CHPIDs associated with the card slot and jack. You can write the cage view to a USB Flash Memory Drive in a printable format.

Select Cage
Select the number of the cage you want to view from **Select Cage** list.

Side View
Select the front or back view radio button from the **Side View** box.

Apply
To apply the changes made to the cage view without closing the window, click **Apply**.

Write to USB Flash Memory Drive
To download the front and back view of the selected cage to a USB Flash Memory Drive, click **Write to USB Flash Memory Drive**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Search

Use the **Search** actions to locate and highlight a specific PCHID assignment or configured CSS.CHPID from the **Channel to PCHID assignment** window.

Enter search text
Enter the PCHID assignment or CSS.CHPID you want to locate.

OK
To locate and highlight a specific PCHID assignment or CSS.CHPID in the **Channel to PCHID Assignment** window, click **OK**.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Channel Problem Determination

Accessing the Channel Problem Determination task

You can use the support element workplace to determine the state and status of specific channel paths in the input/output (I/O) configuration of the central processor complex (CPC). The label for each channel path's icon includes its physical channel identifier (PCHID), state, and status. When you need more detailed information on determining problems, you can use the support element workplace to perform channel problem determination. Perform channel problem determination to get the following types of information, referred to as *problem determination information*, for a channel path:

- Analyze channel information...
- Analyze subchannel data...
- Analyze control unit header...
- Analyze paths to a device...
- Analyze device status...

- Analyze serial link status...
- Display message buffer status...
- Fabric login status...
- Analyze link error statistics block...
- Optical Power Measurement.

If you have experience using other systems, you may have performed *input/output (I/O) problem determination* to get similar information for a channel path.

To perform channel problem determination:

1. Open the **Channel Problem Determination** task.

   The Partition Selection window lists the logical partitions which problem determination can be performed.
2. Select from the list the logical partition that you want to perform problem determination.
3. Click **OK**.

   The Channel Problem Determination window lists the types of problem determination information you can get for the selected channel.

   Note: The channel you selected to start the task is the task's initial input. One or more windows are displayed if additional input is needed to display the type of information you want.
4. Select the radio button beside the type of problem determination information you want, then click **OK**.

   Follow the instructions on each subsequent window, if any, to provide the additional input needed to display the type of information you selected.

   Upon providing the additional input, if any, the channel's problem determination information is displayed.

Check Dependencies

Accessing the Check Dependencies task

The dependencies of internal code changes are designated by support system when the changes are created. After internal code changes are retrieved to the Support Element of the system, their dependencies, if any, are checked automatically whenever you start an operation that will change the system's internal code. Such an operation is attempted only if all dependencies of the internal code changes are met.

You can use the Support Element to also *manually* check the dependencies of internal code changes. Manually checking that dependencies is useful:

- Before you perform an operation for changing the system's internal code.

  By manually checking the dependencies of internal code changes you intend to select while performing the operation, you might get a detailed list of the dependencies that would not be met, but which you must meet before or while actually attempting the operation.

  Note: This is especially important if you intend to use specific internal code changes, rather than all changes, while performing the operation. Using specific changes increases the possibility of *not* specifying one or more dependencies of the specific changes.
- After automatic dependency checking notifies you, upon attempting an operation, that one or more dependencies are not met.

  By manually checking the dependencies of internal code changes you selected while attempting the operation, you get a detailed list of the dependencies that were not met, but which you must meet before or while attempting the operation again.

Ordinarily, only a service representative checks the dependencies of internal code changes, typically while following a service procedure for changing the system's internal code. If you are not following a

service procedure, it is recommended that you check dependencies only with assistance from product engineering, provided through your service representative or support system.

To manually check dependencies:

1. Locate and open the **Check Dependencies** task.
2. Select the radio button that describes the operation and internal code changes for which you want dependencies checked, then click **OK** to begin the dependency checking.
3. Wait until a window indicates the dependency checking is complete. The window also indicates whether all dependencies were met for performing the selected operation:
   - If all dependencies were met, you can return to the service procedure you are following and proceed with its instructions for actually performing the operation.
   - If one or more dependencies were not met, the window lists messages that describe each dependency that was not met, identify the operations you must perform to meet the dependencies, and identify the EC number and change level of each internal code change you can or must use with the operations to meet the dependencies. Upon returning to the service procedure you are following, you can proceed with its instructions and refer to its recovery actions for meeting failed dependencies described by the messages.

   In either case, click **OK** to close the window.

Check Dependencies

Use this window to check whether internal code changes meet all the dependencies that must be met to use them with operations that change the internal code of the console.

Note: Ordinarily, only a service representative checks the dependencies of internal code changes, typically while following a service procedure for changing the console's internal code. If you are not following a service procedure, it is recommended that you check dependencies only with assistance from product engineering, provided through your service representative or support system.

The dependencies of internal code changes are designated by the support system when the changes are created. After internal code changes are retrieved to the console, their dependencies, if any, are checked automatically whenever you start an operation that will change the console's internal code. Such an operation will be attempted only if all dependencies of the internal code changes are met.

This option provides a means for manually checking the dependencies of internal code changes. Manually checking dependencies is useful:

- Before you perform an operation for changing the console's internal code.

  By manually checking the dependencies of internal code changes you intend to select while performing the operation, you may get a detailed list of the dependencies that would not be met, but which you must meet before or while actually attempting the operation.

  Note: This is especially important if you intend to use specific internal code changes, rather than all changes, while performing the operation. Using specific changes increases the possibility of not specifying one or more dependencies of the specific changes.
- After automatic dependency checking notifies you, upon attempting an operation, that one or more dependencies are not met.

  By manually checking the dependencies of internal code changes you selected while attempting the operation, you get a detailed list of the dependencies that were not met, but which you must meet before or while attempting the operation again.

Dependency checking options

To check dependencies of internal code changes manually, select the option that describes the operation and internal code changes for which you want dependencies checked, then click **OK**.

“Install and activate of all changes concurrently” on page 407.
To check the dependencies that must be met to install and activate all internal code changes, select **Install and activate of all changes concurrently**.

“Install and activate of all changes disruptively” on page 408.
To check the dependencies that must be met to install and activate all internal code changes, select **Install and activate of all changes disruptively**.

“Remove and activate of all changes concurrently” on page 408.
To check the dependencies that must be met to remove and activate all internal code changes, select **Remove and activate of all changes concurrently**.

“Remove and activate of all changes disruptively” on page 408.
To check the dependencies that must be met to remove and activate all internal code changes, select **Remove and activate of all changes disruptively**.

“Install and activate of specific changes disruptively” on page 409.
To check the dependencies that must be met to install and activate specific internal code changes, select **Install and activate of specific changes disruptively**.

“Remove and activate of specific changes disruptively” on page 409.
To check the dependencies that must be met to remove and activate specific internal code changes, select **Remove and activate of specific changes disruptively**.

“Install and activate of specific changes concurrently” on page 410.
To check the dependencies that must be met to install and activate specific internal code changes, select **Install and activate of specific changes concurrently**.

“Remove and activate of specific changes concurrently” on page 410.
To check the dependencies that must be met to remove and activate specific internal code changes, select **Remove and activate of specific changes concurrently**.

“Accept specific changes” on page 411.
To check the dependencies that must be met to accept specific internal code changes, select **Accept specific changes**.

OK
To start the dependency checking described by your selection, click **OK**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Install and activate of all changes concurrently

Select the **Install and activate of all changes concurrently** option to check the dependencies that must be met to install and activate all internal code changes concurrently without disrupting its operating system activity.

Selecting this choice checks that dependencies of only the internal code changes that are eligible for being installed and activated concurrently on the system. That is, dependencies will be checked only for internal code changes that were retrieved to the console, but are not currently installed.

The results of dependency checking provide information that may assist you with planning and managing internal code changes. For example:

- If the results indicate all dependencies are met, you can proceed with actually installing and activating all internal code changes.
- If the results indicate not all dependencies are met, you can use the detailed information provided in the results to meet the dependencies before or while actually installing and activating all internal code changes.

  Note: The detailed information identifies the operations and internal code changes you must use to meet the dependencies.

Install and activate of all changes disruptively

Select the **Install and activate of all changes disruptively** option to check the dependencies that must be met to install and activate all internal code changes disruptively by interrupting operating system activity on the system.

Selecting this choice checks that dependencies of the internal code changes that are eligible for being installed and activated, including those that are disruptive on the system. That is, dependencies will be checked only for internal code changes that were retrieved to the console, but are not currently installed.

The results of dependency checking provide information that may assist you with planning and managing internal code changes. For example:

- If the results indicate all dependencies are met, you can proceed with actually installing and activating all internal code changes.
- If the results indicate not all dependencies are met, you can use the detailed information provided in the results to meet the dependencies before or while actually installing and activating all internal code changes.

  Note: The detailed information identifies the operations and internal code changes you must use to meet the dependencies.

Remove and activate of all changes concurrently

Select the **Remove and activate of all changes concurrently** option to check the dependencies that must be met to remove and activate all internal code changes concurrently without disrupting operating system activity on the system.

Automatic dependency checking is performed when you actually attempt to change the internal code of the console by removing and activating all internal code changes. You can use this choice to manually perform the same dependency checking now, without removing and activating the changes or otherwise changing the console's internal code.

Selecting this choice checks that dependencies of only the internal code changes that are eligible for being removed and activated concurrently. That is, dependencies will be checked only for internal code changes that are currently installed.

The results of dependency checking provide information that may assist you with planning and managing internal code changes. For example:

- If the results indicate all dependencies are met, you can proceed with actually removing and activating all internal code changes.
- If the results indicate not all dependencies are met, you can use the detailed information provided in the results to meet the dependencies before or while actually removing and activating all internal code changes.

  Note: The detailed information identifies the operations and internal code changes you must use to meet the dependencies.

Remove and activate of all changes disruptively

Select the **Remove and activate of all changes disruptively** option to check the dependencies that must be met to remove and activate all internal code changes disruptively by interrupting operating system activity on the system.

Automatic dependency checking is performed when you actually attempt to change the internal code of the console by removing and activating all internal code changes disruptively. You can use this choice to manually perform the same dependency checking now, without removing and activating the changes or otherwise changing the console's internal code.

Selecting this choice checks that dependencies of only the internal code changes that are eligible for being removed and activated disruptively. That is, dependencies will be checked only for internal code changes that are currently installed.

The results of dependency checking provide information that may assist you with planning and managing internal code changes. For example:

- If the results indicate all dependencies are met, you can proceed with actually removing and activating all internal code changes.
- If the results indicate not all dependencies are met, you can use the detailed information provided in the results to meet the dependencies before or while actually removing and activating all internal code changes.

  Note: The detailed information identifies the operations and internal code changes you must use to meet the dependencies.

Install and activate of specific changes disruptively

Select the **Install and activate of specific changes disruptively** option to check the dependencies that must be met to install and activate specific internal code changes disruptively by interrupting operating system activity on the system.

Selecting this choice checks that dependencies of only the internal code changes that are eligible for being installed and activated disruptively on the system. That is, dependencies will be checked only for internal code changes that were retrieved to the console, but are not currently installed.

The results of dependency checking provide information that may assist you with planning and managing internal code changes. For example:

- If the results indicate all dependencies are met, you can proceed with actually installing and activating all internal code changes.
- If the results indicate not all dependencies are met, you can use the detailed information provided in the results to meet the dependencies before or while actually installing and activating all internal code changes.

  Note: The detailed information identifies the operations and internal code changes you must use to meet the dependencies.

  Important: Many combinations of specific internal code changes may meet all dependencies for being removed and activated, but it is recommended that you remove and activate all installed internal code changes instead. Using specific changes risks removing and activating an untested combination of changes.

Remove and activate of specific changes disruptively

Select the **Remove and activate of specific changes disruptively** option to check the dependencies that must be met to remove and activate specific internal code changes disruptively by interrupting operating system activity on the system.

Automatic dependency checking is performed when you actually attempt to change the internal code of the console by removing and activating specific internal code changes disruptively. You can use this choice to manually perform the same dependency checking now, without installing and activating the changes or otherwise changing the console's internal code.

Selecting this choice checks that dependencies of only the internal code changes you specify on a subsequent window, if the changes are eligible for being removed and activated disruptively. That is, dependencies will be checked only for specified internal code changes that are currently installed.

The results of dependency checking provide information that may assist you with planning and managing internal code changes. For example:

- If the results indicate all dependencies are met, you can proceed with actually removing and activating the specific internal code changes.
- If the results indicate not all dependencies are met, you can use the detailed information provided in the results to meet the dependencies before or while actually removing and activating the specific internal code changes.

Note: The detailed information identifies the operations and internal code changes you must use to meet the dependencies.

Important: Many combinations of specific internal code changes may meet all dependencies for being removed and activated, but it is recommended that you remove and activate all installed internal code changes instead. Using specific changes risks removing and activating an untested combination of changes.

Install and activate of specific changes concurrently

Select the **Install and activate of specific changes concurrently** option to check the dependencies that must be met to install and activate specific internal code changes concurrently without disrupting system activity on the system.

Automatic dependency checking is performed when you actually attempt to change the internal code of the console by installing and activating specific internal code changes concurrently. You can use this choice to manually perform the same dependency checking now, without installing and activating the changes or otherwise changing the console's internal code.

Selecting this choice checks that dependencies of only the internal code changes you specify on a subsequent window, if the changes are eligible for being installed and activated. That is, dependencies will be checked only for specified internal code changes that were retrieved to the console, but are not currently installed.

The results of dependency checking provide information that may assist you with planning and managing internal code changes. For example:

- If the results indicate all dependencies are met, you can proceed with actually installing and activating the specific internal code changes.
- If the results indicate not all dependencies are met, you can use the detailed information provided in the results to meet the dependencies before or while actually installing and activating the specific internal code changes.

  Note: The detailed information identifies the operations and internal code changes you must use to meet the dependencies.

  Important: Many combinations of specific internal code changes may meet all dependencies for being installed and activated, but it is recommended that you install and activate all retrieved internal code changes instead. Using specific changes risks installing and activating an untested combination of changes.

Remove and activate of specific changes concurrently

Select the **Remove and activate of specific changes concurrently** option to check the dependencies that must be met to remove and activate specific internal code changes concurrently without disrupting system activity on the system.

Automatic dependency checking is performed when you actually attempt to change the internal code of the console by removing and activating specific internal code changes concurrently. You can use this choice to manually perform the same dependency checking now, without installing and activating the changes or otherwise changing the console's internal code.

Selecting this choice checks that dependencies of only the internal code changes you specify on a subsequent window, if the changes are eligible for being removed and activated. That is, dependencies will be checked only for specified internal code changes that are currently installed.

The results of dependency checking provide information that may assist you with planning and managing internal code changes. For example:

- If the results indicate all dependencies are met, you can proceed with actually removing and activating the specific internal code changes.
- If the results indicate not all dependencies are met, you can use the detailed information provided in the results to meet the dependencies before or while actually removing and activating the specific internal code changes.

Note: The detailed information identifies the operations and internal code changes you must use to meet the dependencies.

Important: Many combinations of specific internal code changes may meet all dependencies for being removed and activated, but it is recommended that you remove and activate all installed internal code changes instead. Using specific changes risks removing and activating an untested combination of changes.

Accept specific changes

Select the **Accept specific changes** to check the dependencies that must be met to accept specific internal code changes.

Automatic dependency checking is performed when you actually attempt to change the internal code of the console by accepting specific internal code changes. But you can use this choice to manually perform the same dependency checking now, without accepting the changes or otherwise changing the console's internal code.

Selecting this choice checks that dependencies of only the internal code changes you specify on a subsequent window, if the changes are eligible for being accepted. That is, dependencies will be checked only for specified internal code changes that are currently installed and activated.

The results of dependency checking provide information that may assist you with planning and managing internal code changes. For example:

- If the results indicate all dependencies are met, you can proceed with actually accepting the specific internal code changes.
- If the results indicate not all dependencies are met, you can use the detailed information provided in the results to meet the dependencies before or while actually accepting the specific internal code changes.

  Note: The detailed information identifies the operations and internal code changes you must use to meet the dependencies.

  Important: Many combinations of specific internal code changes may meet all dependencies for being accepted, but it is recommended that you accept all installed and activated internal code changes instead. Using specific changes risks accepting an untested combination of changes.

Checkout Tests

Accessing the Checkout Tests task

Checkout tests are test programs typically run by service representatives to test the central processor complex (CPC) hardware and determine whether it is operating correctly.

Running checkout tests will require all CPC resources. That is, you will not be able to run other control programs or operating systems of the CPC while checkout tests are running.

Checkout tests are fully automated. Once you start them, they require no input or interaction until they are completed. Checkout tests begin with a power-on reset of the CPC and with the diagnostic (D0) input/output configuration data set (IOCDS), followed by loading and running the test programs.

Note: The power-on reset cancels all operations in progress on the CPC, and loading the checkout tests replaces the CPC's current control program or operating system. When the checkout tests are completed, activate the CPC to perform a power-on reset and load the previous control program or operating system.

Checkout tests include testing the CPC's processors and storage, and running internal wrap tests on its channels.

Note: Other hardware in the CPC's input/output (I/O) configuration, such as drivers, receivers, interface cables, control units, and I/O devices, are not tested.

To start checkout tests:

1. Locate and open the **Checkout Tests** task.

2. Click **Run test** from the **Checkout Tests** window to start the checkout tests.

   When checkout tests are completed, the results are displayed. The results provide information about errors that were detected or problems that occurred, if any, during testing.

Choose a Disconnected Session

Choose a Disconnected Session

This window appears when you have logged back on to the console after previously disconnecting. A list of disconnected sessions is displayed for the specified user.

List of disconnected sessions
This list displays the sessions that have been previously disconnected by the specified user ID.

Session Id
Specifies the identification number associated with the disconnected session.

Disconnect Time
Specifies the time the session was disconnected.

Creation Time
Specifies the time the session originally started.

Running Tasks
Specifies the number of tasks that are currently running in that session.

Reconnect
To reconnect to the session you have selected in the list, click **Reconnect**.

New Session
To connect to a new session rather than a session that has been disconnected, click **New Session**.

Delete
To delete a disconnected session that you no longer need to work with, click **Delete**.

Note: If you delete the last disconnected session from the list, you will be immediately logged on with a new session since there are no longer any disconnected sessions to choose.

Cancel
To close this window and return to the welcome window without connecting, click **Cancel**.

Help
To display help for the current window, click **Help**.

Cleanup Discontinuance

Cleanup Discontinuance

This task halts the discontinuance process started by the **Prepare for Discontinuance** task if it is run before the system is rebooted. However, the Capacity on Demand records removed by the **Prepare for Discontinuance** task will not be restored.

Common Targeting

Common Targeting

Use this window to perform an action on a selected target object.

Click a menu option to select an action you want to perform on the target object. Detailed help is available when a target object and action are selected.

Click **Refresh** to redisplay the selection list.

Configure On/Off

Accessing the Configure On/Off task

Configure on and *configure off* are channel path operations you can use to control whether channel paths are online or on standby in the active input/output (I/O) configuration:

- A channel path is *online* while configured on. It is in the active I/O configuration and it can be used.
- A channel path is on *standby* while configured off. It is in the active I/O configuration but it cannot be used until it is configured on.

If you have experience using other systems, you may have used a CHPID command with ON and OFF parameters to configure channel paths on and off.

You can use this task to configure channel paths on or off. However, operating systems will not be notified when you use the workplace to configure channel paths on or off. For example, if you configure off a channel path, the operating system running in any image that owns or shares the channel path is not notified, and the next operation from the operating system to the channel path causes an error. It is recommended you use the operating system facilities rather than the Support Element workplace, whenever possible, to configure channel paths on and off.

Notes:

- When using z/OS® operating environment, deactivate the crypto through ICSF before configuring off crypto. To determine when crypto initialization has completed after a configure on or a crypto, see the **Cryptographic Configuration** task.
- Depending on your user task role, you may only be able to view this task.

To use the workplace to configure a channel path on or off:

1. Open the **Configure On/Off** task.

   The Configure On/Off window displays. The window displays the *current state* and *desired state* of the selected object.
2. Use the window list and actions to *toggle* the desired states of the object you want to configure on or off.

   - If the current state of the object is **Online**, toggle its target state to **Standby** if you want to configure off the object.
   - If the current state of the object is **Standby**, toggle its target state to **Online** if you want to configure on the object.

   Note: If you attempt to change the target state of an object that cannot be configured on or off, a message is displayed in the **Messages** list column to indicate changing the object is not allowed. Click on the message for more information about why the object state cannot be changed.
3. When you finish changing the target states of the object you want to configure on or off, click **OK** to make each object new target state its current state.

Configure On/Off

This window can be used to determine if channel path, crypto, or function ID (FID) can be configured on or off for a Central Processor Complex (CPC) image. For some user task roles the window can be used to configure the channel path, crypto, or FID on or off. Configuring channel paths, crypto, or FID on and off controls whether they are online or on standby in the active Input/Output (I/O) configuration:

- A channel path, crypto, or FID is *online* while configured on. It is in the active I/O configuration, and it can be used.
- A channel path, crypto, or FID is on *standby* while configured off. It is in the active I/O configuration, but it cannot be used until it is configured on.

Notes:

1. Operating systems will *not* be notified when you use this window to configure a channel path, crypto, or FID on or off. For example, if you use the window to configure off a channel path, the operating system running in any image that owns or shares the channel path is not notified, and the next operation from the operating system to the channel path will cause an error. Therefore, whenever possible, it is recommended that you use operating system facilities rather than the **Configure On/Off** task to configure channel paths on and off.
2. When the CPC is activated in logically partitioned (LPAR) mode, configuring off a reconfigurable channel path does *not* release it from its assignment to an isolated logical partition.
3. When the CPC is activated in LPAR mode, the **Online pending** state indicates the channel path was configured on while assigned to an inactive logical partition. The channel path will be online when the logical partition is activated.
4. This task may be view only for some user task roles.

To use the **Configure On/Off** task:

- The CPC must be power-on reset.

Additional functions on this window include:

OK

When you finish toggling the target states of the channel path, crypto, or FID you want to configure on or off, click **OK** to allow the new target states to take effect.

Cancel

To close the Configure On/Off window, click **Cancel**.

Help

To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Configure on/off table

The window lists the following information for each PCHID, channel path, crypto, or FID targets you selected to start the task. The information displayed depends on what object is selected. Selecting a PCHID shows the PCHID number in the first column. Select **Toggle** from the drop down box to toggle their target states.

PCHID

Displays a four-digit physical channel identifier (PCHID) associated with the selected channel path, crypto, and FID.

ID

Displays the ID for the selected channel path, crypto, or FID.

LPAR Name

Displays the logical partition name for the selected channel path, crypto, and FID.

Current State

Indicates the current state of each channel path, crypto, or FID.

Desired state

Indicates the target state of each channel path, crypto, or FID.

Messages

If you attempt to change the target state of a channel path, crypto, or FID that cannot be configured on or off, this column displays the message "Not Allowed" for the channel path, crypto, or FID to indicate that changing its state is not allowed.

The icons perform the following functions for the selected configure on/off table:

Select All/Deselect All

You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired

block and then shift-clicking the selection box of the last row in the desired block. Click **Select All** or **Deselect All** to select or deselect all objects in the table.

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want.

Clear All Filters
Click **Clear All Filters** to return to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Current State

This window lists the current state and target of each PCHID, channel path, crypto, or FID target you selected to start the task. Use the select action drop down to *toggle* the target states of the channel paths, cryptos, or FIDs you want to configure on or off.

- If the current state of a channel path, crypto, or FID is **Online** or **Online pending,** toggle its target state to **Standby** if you want to configure off the channel path, crypto or FID.
- If the current state of a channel path, crypto, or FID is **Standby,** toggle its target state to **Online** if you want to configure on the channel path, crypto, or FID.

Online
Indicates the channel path, crypto, or FID is configured on. It is in the active Input/Output (I/O) configuration and it can be used.

Online pending
When the Central Processor Complex (CPC) is activated, this state indicates the channel path, crypto, or FID was configured on while assigned to an inactive logical partition. The channel path, crypto, or FID will be online when the logical partition is activated.

Reserved - Service
Indicates the channel path, crypto, or FID has service set on. It is not in the active I/O configuration, cannot be configured on, and cannot be used. It will remain out of the active I/O configuration until service is set off.

Reserved
Indicates the channel path, crypto, or FID has service set off. A CHPID can be in the reserved state if it is not defined or incorrectly defined in the active IOCDS.

Standby
Indicates the channel path, crypto, or FID is configured off. It is in the active I/O configuration but it cannot be used until it is configured on.

Console Default User Settings

Accessing the User Settings task

Notes:

- Only a user ID assigned access administrator roles sets the defaults of the Support Element console settings by using the **Console Default User Settings** task.
- Because there are many main users interfaces (one for each logged on user), the Support Element console provides each user the ability to change settings. In other words, if you change confirmation settings or controls, this does not cause that same change for other logged-on users.

This task enables you to customize settings that control how the Support Element console operates. You can choose settings such as: single object selection, show tips, or choose when to display or not display confirmation windows.

User Settings

Use the **User Settings** task to customize settings that control how you want the console to operate for your user ID.

User Settings tabs

Use these tabs to control how you want the console to operate for your user ID.

"Confirmations" on page 416
To customize your preferences for using confirmation windows for a subset of console workplace tasks, select the **Confirmations** tab.

"Controls" on page 417
To select the object controls that you prefer, select the **Controls** tab.

Additional options are available from these pages:

Apply
To save the settings currently displayed on this tab, click **Apply**.

Reset
To discard any changes you made to the settings on this tab, and display again the current settings for this window, click **Reset**. If changes have been saved by clicking **Apply**, you can no longer discard the changes.

Defaults
To return to the preferences on this tab to the settings that are the default for the current user, click **Defaults**.

Note: If you are using this option from the **Console Default User Settings** task, then you are returning to the preferences on this tab to the settings that are the system default for all users.

OK
To save the settings on all tabs, click **OK**.

Cancel
To exit this window without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Confirmations

Use this page to customize preferences for using confirmation windows for a subset of tasks.

The preferences you set for using confirmation windows apply to the following subset of tasks:

- Activate
- Deactivate
- Load
- Start
- Start All Processors
- Stop
- Stop All Processors

You can customize the console for displaying a confirmation window upon starting any of the tasks listed above. A confirmation window identifies the task and, optionally, lists the task's target objects.

The console operator must use a confirmation window either to confirm starting the task or to cancel it instead.

Confirmation windows reduce the possibility of inadvertently performing tasks, particularly tasks that may disrupt the operation of the Central Processor Complex (CPC) or its images.

Customize the settings to indicate your preferences, then click **Apply**.

Enabled with object list
To display a confirmation window upon starting any of the tasks listed above and to list the task's target objects, select **Enabled with object list**.

Note: The **Load** task does not support this option.

Enabled without object list
To display a confirmation window upon starting any of the tasks listed above, but without listing the task's target objects, select **Enabled without object list**.

Do not show confirmations
To start the tasks listed above without displaying confirmation windows, select **Do not show confirmations**.

Use 'No' as the default action
To set the confirmation window's default action to 'No' upon starting any of the tasks listed above, select **Use 'No' as the default action**.

- If this is selected (a check mark appears) it indicates the default action for the confirmation window is to cancel the task. That is, the **No** button is preselected on the confirmation window, click **No** to cancel the task.
- If this is not selected (a check mark does not appear) it indicates the default action for the confirmation window is to confirm starting the task. That is, the **Yes** button is preselected on the confirmation window, click **Yes** to confirm starting the task.

Controls

Use this page to select the object controls to use on the console.

Single object selection
To select only one object at a time while working on a task, select **Single object selection**. Otherwise, more than one object can be selected while working on a task.

Accept Console Messenger messages
To allow your console sessions to receive Console Messenger chat and broadcast messages, select **Accept Console Messenger messages**. Otherwise, your sessions will not receive these messages, and other sessions attempting to initiate chats with your session will be told that you have elected not to participate in chats.

Note: This option is not available when the Console Messenger facility is disabled. To enable the Console Messenger facility, go to the **Customize Console Services** task.

Bring Chat Window to foreground on new message
The initial chat message window is always displayed in the foreground to notify you of the incoming chat message.

To have the Console Messenger task continue to bring an open chat message window to the foreground after the initial message is received, select **Bring Chat Window to foreground on new message**.

Note: This option is not available when the Console Messenger facility is disabled. To enable the Console Messenger facility, go to the **Customize Console Services** task.

Display timestamps using
To define the time zone that is used to localize timestamps, for those tasks that use timestamps. Select the drop-down arrow to choose your preference.

Notes:

- This is only available for those tasks that are enabled to respect this timestamp setting.
- From the **User Settings** task, if you change your preference and apply this change, a message appears indicating you must restart your login session before the change appears.

Client Time Zone
To display timestamps localized to the time zone of the client browser, select **Client Time Zone**. If you are on a local session, this is the same as the Console Time Zone.

Console Time Zone
To display timestamps localized to the time zone of the Support Element, select **Console Time Zone**. This is the default. If you are on a local session, this is the same as the Client Time Zone.

UTC Time Zone
To display timestamps localized to the UTC time zone, select **UTC Time Zone**.

Console Default User Settings

Use the **Console Default User Settings** task to set the default settings for operating the console.

Only the ACSADMIN default user ID or a user ID with access administrator roles can access this task.

This task will not affect currently logged on users until they log off then log back on.

Console Default User Settings tabs

Use these tabs to set the defaults for controlling how the console operates for all users.

"Confirmations" on page 416
To set preferences for using confirmation windows for a subset of console workplace tasks, select the **Confirmations** tab.

"Controls" on page 417
To set the object controls, select the **Controls** tab.

Additional options are available from these pages:

Apply
To save the settings currently displayed on this window, click **Apply**.

Reset
To discard any changes you made to the settings on this window, and display again the current settings for this window, click **Reset**.

Defaults
To return to the preferences that are the default for the current user, click **Defaults**.

OK
To save the settings, click **OK**.

Cancel
To exit this window without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Console Messenger

Accessing the Console Messenger task

Note: To send messages using this task, you must enable **Console messenger** from the **Customize Console Services** task. Enabling **Console messenger** also allows you to receive messages. The **Accept Console Messenger messages** and **Bring Chat Window to foreground on new message** options become available from the **Controls** tab of the User settings task to allow you to customize the way that this task operates for your user ID.

Use this task to provide a simple person-to-person message communication facility between users of the Support Element and Hardware Management Console.

You can send a broadcast message or you can initiate a two-way chat.

Sending a broadcast message

This function allows you to send the same information to all the users on a console at the same time. To send a broadcast message:

1. Open the **Console Messenger** task. The Console Messenger window is displayed. This window allows you to choose the console or user that you want to send a message to and whether or not you want to send a two-way chat or send a broadcast message.
2. To send a broadcast message, select a top level console from the ***Reachable Consoles*** tree view list section of the window and make sure **Broadcast** is displayed in the ***Message Type*** section of the window.
3. Click **OK**. The Send Broadcast Message window is displayed.

   This window indicates who the recipient of your message will be and includes a message area for you to provide information that will be sent to all other user sessions (logged on and disconnected) of the selected console.
4. Specify a message in the **Message** input field, then click **Send**. The Broadcast Message Sent window is displayed indicating whether or not your message was received successfully.
5. Click **Close** to return to the Support Element console workplace.

If you are receiving a broadcast message, the Broadcast Message Received window is immediately displayed on your Support Element console. This window identifies the user that sent the message and displays the message sent by the user.

From this window you can:

- View more information about where the message came from, click **view more info**.
- Begin a two-way chat session with the user session that sent the broadcast message, click **Initiate® Chat**.
- End the task and return to the Support Element console workplace, click **Close**.

Initiating a two-way chat

This function allows you to send a message to an individual user. To initiate a two-way chat:

1. Open the **Console Messenger** task. The Console Messenger window is displayed. This window allows you to choose the console or user you want to send the message to and whether or not you want to send a two-way chat or send a broadcast message.
2. To send a two-way chat, select an individual user session located below the reachable console. This automatically changes the ***Message Type*** area to **Two-way Chat**, then click **OK**. The Console Messenger Chat window is displayed.

   This window indicates who you will be sending messages to, a history of the dialogue you will be having with your chat partner, and a message area for you to provide information that will be sent to your chat partner.
3. Specify a message in the **Message** input field, then click **Send**. The Console Messenger Chat window is refreshed with the message you entered now appearing in the **History** area of the window with the prefix **Me**.

   The message is sent to the partner and their Console Messenger Chat window is also refreshed, with the message text appearing in the **History** area with the prefix **Partner** added to it.
4. If both partners need to continue sending messages to each other, specify a message in the **Message** input field and click **Send**.

Note: To ensure that chat window comes to the foreground in your Support Element console sessions when partners send you messages, select **Bring chat window to foreground on message arrival.** (a check mark is displayed).

5. When you are done conversing with your chat partner, click **Close**.

   Note: The **Status** for your chat partner changes to **Closed by partner** and the **Send** option is no longer enabled, indicating that you have closed the Console Messenger Chat window.

There are other Support Element console tasks, such as the **Users and Tasks** task, that offer an ability to open the **Console Messenger** task to start a two-way chat or send a broadcast message. The steps necessary to open the **Console Messenger** task from these other tasks is mentioned in the description of those tasks. Once the **Console Messenger** task has been opened, continue with the steps described in this section for information on the procedure for sending a broadcast message or conducting a two-way chat.

Console Messenger

This task is used to provide a simple person-to-person message communication facility between users of the Hardware Management Console and Support Element.

Note: To initiate this task you must enable **Console messenger** from the **Customize Console Services** task and **Accept Console Messenger messages** must be selected from the **Controls** tab of the **User Settings** task to be able to receive messages.

Instances of this task will also be started automatically in a user's session in order to participate in a two-way chat requested by another user, or to display a broadcast message sent by another user.

Use this window to select the console and user session you want to interact with and what type of interaction is appropriate: a two-way chat or a one time broadcast message.

A console user is able to send messages to users on:

- Any Hardware Management Console that is managing this console
- Any Hardware Management Console that is acting as this console's call-home server.

Reachable Consoles and Message Type

The list of reachable consoles is displayed in a two-level tree view format. The top level of the tree (indicated by the +/- expansion box) contains an entry for each of the reachable consoles (console nodes) that have been identified by this task. The next level in the tree view displays the list of user sessions (either logged on or disconnected) that were running on the console at the time this window was displayed.

Note: A disconnected session is displayed in red and a logged on user is displayed in green. Messages can be sent to disconnected users.

Current Console
Represents the console from where the task is being initiated. It is always displayed at the top of the tree view.

User Session
Appears below the console node and consists of the user's user ID followed by the location from which they initiated the console session.

Selecting from the reachable consoles list determines whether a two-way chat or broadcast message will be initiated. The **Message Type** area changes dynamically according to the selection you have made in the **Reachable Consoles** tree view.

Two-way Chat
Selecting a user session begins a two-way chat with the selected logged on user.

Broadcast
Selecting a console node sends a broadcast message to all of the logged on users of the selected console.

To send a broadcast message to all of the users on any other console that also acts as a managing console for the selected console, select **In addition, send the message to all managing consoles.** Otherwise, the broadcast message is just sent to the users on the selected console node. This option may not be available if the selected console entry does not represent a console that is not managed by others.

Note: There is a possibility that some of the managing consoles may not receive the broadcast message. When you send the broadcast message the **Omitted Consoles** window is displayed. This window lists the managers of the selected consoles that do not have the console messenger facility enabled, therefore those consoles would not receive the message. You can decide whether or not to proceed with the message. **Yes** continues with the message, otherwise **No** cancels sending the message.

Note: The data for the list of available console nodes is obtained when this window is first displayed and is not refreshed. To refresh this data you must cancel the task and re-open it. Also, if the console node is expanded you can refresh that node by collapsing and then re-expanding the node.

Additional options on this window include the following:

OK
To initiate the two-way chat or broadcast message, click **OK**.

Cancel
To exit this task without sending any messages, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Console Messenger Chat

Use this window to engage in a two-way chat with a selected partner, sending messages to the partner and seeing the messages sent by the partner.

Chat Partner
This area of the window displays your chat partner's user ID and the current chat partner session status. The session status information is updated dynamically as it changes. Session status information can be one of the following:

Logged on
Chat session is open and your chat partner is currently logged on.

Disconnected
Chat session is open but your chat partner has disconnected their browser from the console session. The chat session is available for use and your chat partner will see the new messages when they reconnect to the console session.

Closed by partner
Chat partner has closed the chat session. This window remains open for you but new messages cannot be sent.

Partner is no longer reachable
Chat session has been closed because some communication interruption has made message delivery to the chat partner unavailable. This window remains open but new messages cannot be sent.

To see additional information about your chat partner, click **view more info**. The **Chat Partner** area is expanded to display the full user ID and additional console session information, such as start time and the internal session ID. You can restore this area to its original display by clicking **close**.

History
This area of the window is a scrollable text output area that provides a running transcript of the chat session. It displays the messages that you sent, along with the messages that have been received from your chat partner.

The entries in the history area are prefixed with an indication as to who sent the message and the local time the message was sent or received. The prefix is one of the following:

Me
Represents messages that you sent and initiated.

Partner
Represents messages that are received from your chat partner.

The messages are displayed in different colors to allow for easy identification.

In addition to message entries, this area includes marker lines that associate dates with the entries in the history. A date (and time) marker line is placed at the top of this area to record the date on which the chat session started. Additional marker lines are placed in this area any time the history spans a date change boundary, such as crossing midnight.

Message
This area of the window is the input area where you specify the message you want sent to your chat partner.

To send the message to your chat partner you can either, click **Send** or press **Enter**.

Note: The Message area is disabled if the status of your chat partner changes to **Chat Closed** or **Partner Not Reachable**.

Bring chat window to foreground on message arrival.
To bring this window into the foreground when a new message from your chat partner arrives, select **Bring chat window to foreground on message arrival.**

Send
To send the message that you specified in the **Message** input area to your chat partner, and to clear the input area for the next message, click **Send**.

Close
To close the chat and end this task click **Close**. A message is sent to your chat partner indicating the chat session has closed.

Help
To display help for the current window, click **Help**.

Send Broadcast Message

Use this window to send a message to the selected console node.

Recipient
This area of the window lists the console or consoles that the broadcast message is going to be sent. It will always list the name of the console node that you selected from the **Reachable Consoles** list. Also, if you selected the option to send the message to all managing consoles then those consoles would also be included.

Message

This area of the window is the input area where you specify the message you want sent to all of the user sessions on the consoles listed in the **Recipient** area.

To send the broadcast message, click **Send**.

Send
To send the broadcast message that you specified in the **Message** input area to all of the user sessions on the consoles listed in the **Recipient** area, click **Send**.

Once you have sent the message, the **Broadcast Message Sent** window is displayed. This window summarizes the results of sending the broadcast message. It lists the console names that successfully received the broadcast message and those consoles that did not (if applicable). This is an informational window, click **Close** when you have finished reviewing this information.

Cancel
To cancel sending the broadcast message and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Broadcast Message Received

You can use this window to view the message sent to your console or to respond to the message sent to your console.

From
This area of the window displays information about the user session that sent the broadcast message.

To see additional information about your user that sent the message, click **view more info**. The **From** area is expanded to display the location and additional console session information, such as start time and the internal session ID. You can restore this area to its original display by clicking **close**.

Message
This area of the window displays the contents of the broadcast message and the date and time the message was sent.

Initiate Chat
To begin a two-way chat session with the user session that sent the broadcast message, click **Initiate Chat**.

The **Console Messenger Chat** window is displayed.

Close
To close the window and end the task, click **Close**.

Help
To display help for the current window, click **Help**.

CP/SAP Details

CP/SAP Details

This window displays the current instance and acceptable status settings for the selected central processor (CP).

- Instance information includes the current status of the central processors (CPs).
- Acceptable status determines which of the CP statuses are acceptable and which statuses are unacceptable. The support element console reports when the CP status becomes unacceptable.

  Review the settings, then click **Apply** to change the acceptable status settings.

You can find more detailed help on the following elements of this window:

Instance Information

Displays the current instance information for the selected central processor (CP).

Instance Information includes the current status of the CP.

You can find more detailed help on the following elements:

Status

Displays the current status of the CP.

Acceptable status

Displays the current acceptable status settings for the central processor (CP). *Acceptable status settings* determine which of the CP statuses are acceptable and which statuses are unacceptable. To change the settings:

- A check mark indicates an acceptable status.
- Otherwise, no check mark indicates an unacceptable status.

- To change one setting to the other, click once.

The support element console continuously monitors the statuses of the CP and compares them to the CP's acceptable status settings.

While the statuses are acceptable, the background of the CP icon has no color. An *exception* occurs when a status becomes unacceptable. The console reports an exception to the console operator by changing the background color of the CP to the color set for indicating its specific unacceptable status. The color displayed to the right of each status is the color currently used for the background color of the CP when the status is the cause of an exception. That is, the color set for a status is displayed only when the status is unacceptable and it is the current status of the CP.

Note: To change the color set for a status, open the **Console Actions** view, then open **Support Element Settings** from the work area.

Setting the CP's acceptable status settings allows you to control which statuses are reported as exceptions:

- Acceptable statuses, indicated by a check mark, are not reported as exceptions.
- Unacceptable statuses, indicated by no check mark, are reported as exceptions.

You can find more detailed help on the following elements:

Operating

The CP is operating.

Not Operating

The CP is not operating.

The following CP statuses are summarized as not operating:

- Checked stopped
- Loading
- Recovering
- Reset active
- Stepping
- Stopped

Save as default

To allow you to change the acceptable status for all of the current objects defined with the same status type, select **Save as default**. After you click **Apply**, a message window appears confirming that you want to proceed with this operation.

Apply

To apply changes you made to the CP's acceptable status settings, click **Apply**.

Cancel

To close the window without saving changes you made to the CP's acceptable status settings, click **Cancel**.

Help

To display help for the window or its controls, click **Help**.

Cryptographic Configuration

Accessing the Cryptographic Configuration task

The Crypto Express are orderable features.

- The Crypto Express (CCA Coprocessor, EP11 Coprocessor, and Accelerator) features work with the Integrated Cryptographic Service Facility (ICSF) and the Resource Access Control Facility (RACF®) (or equivalent software products) in an z/OS or OS/390® operating environment to provide data privacy, data integrity, cryptographic key installation and generation, electronic cryptographic key distribution, and personal identification number (PIN) processing.
- The cryptographic functions of the Crypto Express Accelerators provide:
  - SSL acceleration of modular arithmetic operations; mainly clear-key RSA private key decryption.
  - A function reduced, but performance enhanced alternative to the CCA Coprocessor and EP11 Coprocessor.
- The cryptographic functions of the Crypto Express Coprocessors provide:
  - Support for CCA (Common Cryptographic Architecture) APIs.
  - Support for AES, DES, and RSA cryptographic operations for data confidentiality, and data integrity and distributed key management.
- Using the cryptographic functions of the Crypto Express EP11 Coprocessor provides:
  - Support for Enterprise PKCS #11 (EP11) APIs.
  - Support secure PKCS #11 keys, keys that never leave the secure boundary of the coprocessor unless encrypted.

This task allows you to monitor the installed Crypto Express features by loading their configuration data during CPC activation. Upon completing the configuration and initialization of the installed Crypto Express features, you can monitor and manage it by:

- Checking the status and details of the Crypto Express features.
- Testing the random number (RN) generators of the Crypto Express CCA Coprocessor.
- Run Customer Initiated Selftest of the Crypto Express EP11 Coprocessor.
- Manually clear the cryptographic keys from the Coprocessor or Accelerator.
- Manually clear the cryptographic keys within the given usage domain(s).
- Import and activate a UDX file configuration.
- Indicate whether to permit TKE commands for processing on the selected Crypto Express CCA Coprocessor.
- Select the crypto configuration type for your system.

To work with the Crypto Express features:

Note: Depending on your user task role, you may only be able to view this task.

1. The Crypto Express features must be installed, and the CPC must be powered-on.
2. Open the **Cryptographic Configuration** task.

The Cryptographic Configuration window lists the Crypto Express features installed in the CPC and provides controls for working with them.

Cryptographic Configuration

Use this window to configure and monitor the Crypto Express features installed in your system. The Crypto Express features can be configured to operate as CCA Coprocessor, EP11 Coprocessor, or Accelerator.

Note: Depending on your user task role, you may only be able to view this task.

The Crypto Express features are secure, integrated hardware that perform high-speed cryptographic functions. Each Cryptographic adapter is identified by a cryptographic number, starting at 0. The cryptographic numbers that can be configured on the system can have an upper limit of 60, but could be smaller depending on your model.

Using the cryptographic functions of the Crypto Express Accelerators provide:

- SSL Acceleration of modular arithmetic operations; mainly, clear-key RSA private key decryption.
- A function reduced, but performance enhanced alternative to the CCA Coprocessor and EP11 Coprocessor.

Using the cryptographic functions of the Crypto Express CCA Coprocessors provide:

- Support for Common Cryptographic Architecture (CCA) APIs.
- Support for AES, DES, and RSA cryptographic operations for data confidentiality, and data integrity and distributed key management in a secure environment.

Using the cryptographic functions of the Crypto Express EP11 Coprocessors provide:

- Support for Enterprise PKCS #11 (EP11) APIs.
- Support secure PKCS #11 keys, keys that never leave the secure boundary of the coprocessor unless encrypted.

Using the cryptographic functions of the Crypto Express features require either:

- Activation of the partition with the crypto settings in your activation profile using the **Customize/Delete Activation Profile** task.
- Changing the crypto settings on the logical partition using the **Change LPAR Cryptographic Controls** task.

Use the Cryptographic Configuration window to start these tasks. You can use this window to perform tasks for configuring and monitoring the Crypto Express features:

- Checking the status and details of the Crypto Express features by clicking View Details....
- Testing the Random Number (RN) generator of the Crypto Express CCA Coprocessors by clicking “Test RNG/CIS” on page 428.
- Run Customer Initiated Selftest of the Crypto Express EP11 Coprocessor by clicking “Test RNG/CIS” on page 428.
- Manually clear the cryptographic keys from the Coprocessor or Accelerator by clicking Zeroize.
- Manually clear the cryptographic keys within the given usage domain(s) by clicking “Domain Management” on page 431.
- Indicate whether to permit TKE commands for processing on the selected Crypto Express CCA Coprocessors by clicking TKE Commands.
- Indicate the crypto type configuration for the Crypto Express features by clicking Crypto Type Configuration.
- Import and activate a UDX file configuration by clicking UDX Configuration.

Number
Displays the ID number assigned by the system to identify the Crypto Express features.

Status
Indicates the status of the Crypto Express feature card; such as, operating or deconfigured.

Crypto Serial Number
Displays the serial number of the crypto adapter contained in the Crypto Express features.

Type
Indicates whether the Crypto Express cryptographic card is configured to operate as a CCA coprocessor, EP11 coprocessor, or an accelerator.

Operating Mode
Displays the operating mode for the Crypto Express features.

TKE Commands
Indicates whether TKE commands are permitted or denied for the Crypto Express features

You can work with the tables by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears. The icons perform the following functions in the crypto table:

Select All
Selects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Deselect All
Deselects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header to change from ascending to descending order. Click **OK** when you have defined your preferred order.

Show Filter Row

Defines a filter for a table column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the check box next to the filter that you want in the filter row.

Clear All Filters

Returns to the complete table summary. The table summary includes the total number of items that pass the filter criteria and to the total number of items.

Clear All Sorts
Returns the table back to the default order.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Refresh
To update the displayed cryptographic configuration information with the current configuration, click **Refresh**.

Cancel
To exit the current task, click **Cancel**.

Help
To display help for the current window, click **Help**.

View cryptographic details

You can use the Support Element workplace to monitor the status of the Crypto Express features.

To view the status of the Crypto Express features:

1. Open the **Cryptographic Configuration** task in system programmer or service representative role..

   The Cryptographic Configuration window lists the Crypto Express features installed in the CPC and provides controls for working with them.

   Note: The Crypto Express features have completed its initialization when the status indicates *Configured*. After initialization is complete, you need to refresh the Cryptographic Configuration window. If initialization is ongoing, you may need to refresh the Cryptographic Configuration window to see the current status until *Configured* is indicated.
2. Select from the list the Crypto Express features that you want more information for.
3. Click **View Details**.

The Cryptographic Details window displays information on the selected Crypto Express features.

Test RNG/CIS

Use this task to:

- Verify whether the Random Number (RN) generated of the Crypto Express CCA Coprocessor are sufficiently random. Ordinarily, a RN generator is tested automatically when it is initialized, but you can use this task to manually test an RN generator. You can select to run a RN generator test on individually selected Crypto Express CCA Coprocessors or run a test on all Crypto Express CCA Coprocessors.
- Run a Customer Initiated Selftest of the Crypto Express EP11 Coprocessors.

To test a Crypto Express CCA Coprocessor or EP11 Coprocessors:

1. The Crypto Express CCA Coprocessors or EP11 Coprocessors must be online and assigned to a logical partition.
2. Open the **Cryptographic Configuration** task in system programmer or service representative role.

   The Cryptographic Configuration window lists the Crypto Express features installed in the CPC, and provides buttons for working with them.

   To manually test specific Crypto Express CCA Coprocessors or EP11 Coprocessors:

   - Select from the list a configured Crypto Express CCA Coprocessors or EP11 Coprocessors that you want to test.
   - Click **Test RNG/CIS** to test them.

     A message is displayed to indicate the results of the test.

   To manually run the test on **all** Crypto Express CCA Coprocessors or EP11 Coprocessors:

   - Use the **Select All** function from the table icons or **Select Action** list from the table tool bar and to test all.

     A message is displayed to indicate the results of the test.

Zeroize Coprocessors or Accelerators manually

Zeroizing a Coprocessor or Accelerator for the Crypto Express features clear all configuration data and cryptographic keys by resetting them to binary zeroes.

Attention: Zeroizing one or all Coprocessors or Accelerators clears its configuration data and clears all cryptographic keys. Zeroizing all also erases configuration data from the Support Element hard drive (for example, UDX files). The selected Coprocessor or Accelerator should be zeroized manually only when absolutely necessary, typically when the Coprocessor or Accelerator configuration data must be erased completely.

For example:

- You must zeroize selected Coprocessors or Accelerators prior to selling or transferring ownership of the CPC.
- A service representative may zeroize Coprocessors or Accelerator prior to upgrading the CPC, if required.
- You may want to zeroize selected Coprocessors or Accelerators if, in an emergency, it is the only way to maintain the security of encrypted data.

To manually zeroize Crypto Express CCA Coprocessors or EP11 Coprocessors:

1. A power-on reset of the CPC must be complete.
2. The Crypto Express CCA Coprocessor or Crypto Express EP11 Coprocessor must be online and assigned to a logical partition.
3. Open the **Cryptographic Configuration** task in system programmer or service representative role.

   This displays the Cryptographic Configuration window. The window lists the Coprocessors and Accelerators installed on the CPC, and provides controls for working with them.

To manually zeroize a specific :

- Select from the list the configured Coprocessor or Accelerator you want to zeroize.
- Click **Zeroize** to zeroize the selected Coprocessor or Accelerator.

  A Zeroize Warning window is displayed to notify you of the consequences for clearing the configuration data.
- Click **Zeroize** to confirm your request to zeroize the selected Coprocessor or Accelerator.

To manually run zeroize on all Coprocessors or Accelerators:

- Click **Zeroize All** to zeroize all the Coprocessors and Accelerators and erase configuration data from the Support Element hard drive.

  A Zeroize Warning window is displayed to notify you of the consequences for zeroizing all the Coprocessors and Accelerators.
- Click **Zeroize All** to confirm your request to zeroize them.

A message is displayed to indicate the results of the function.

Domain Management

Zeroizing a usage domain clears the cryptographic keys for a selected logical partition by resetting them to binary zeroes.

To zeroize a logical partition usage domain:

1. A power-on reset of the CPC must be complete.
2. The Crypto Express CCA Coprocessor or EP11 Coprocessor must be online and assigned to a logical partition.
3. Open the **Cryptographic Configuration** task in system programmer or service representative role.

   This displays the Cryptographic Configuration window. The window lists the Crypto Express CCA Coprocessors or EP11 Coprocessor installed in the CPC, and provides controls for working with them.

   To zeroize a usage domain:

   - Select from the list the configured Coprocessor you want to zeroize.
   - Click **Domain Management**.

     A Domain Management window is displayed
   - Select the usage domain index(es) to zeroize.
   - Click **Zeroize** to confirm your request to zeroize the selected usage domain indexes.

   A message is displayed to indicate the results of the function.

TKE commands

The TKE workstation can manage secure functions of a specific Crypto Express CCA Coprocessors only if permission is given. If permission is denied, all requests for information or commands to a specific Crypto Express CCA Coprocessors from the TKE workstation will not be allowed. You can use the Support Element to dynamically permit or deny TKE commands to the Crypto Express CCA Coprocessors from the TKE workstation.

Note: Permitting TKE access with the default TKE communication keys set can allow unauthorized access. For security reasons you should immediately change the default value of the keys from the TKE.

To permit or deny TKE commands:

1. The Crypto Express CCA Coprocessors must be online and assigned to a logical partition.
2. Open the **Cryptographic Configuration** task in system programmer or service representative role.

   The Cryptographic Configuration window lists the Crypto Express CCA Coprocessors installed in the CPC and provides controls for working with them.

3. Select from the list the Crypto Express CCA Coprocessors that you want to view or modify TKE command permission.
4. Click **TKE Commands**.

   The TKE Commands Configuration window displays information on the TKE commands for the selected Crypto Express CCA Coprocessors.
5. Select the Crypto Express CCA Coprocessors to permit or deny TKE commands. The check box displays a check mark when you mark it.
6. **Permit**
   To permit TKE commands, click **Permit**.

   Deny
   To deny TKE commands, click **Deny**.

Crypto type configuration

The selected Crypto Express (CCA Coprocessors, EP11 Coprocessors, and Accelerators) features can be configured to run as an accelerator or coprocessor. The selected Crypto Express features must be deconfigured prior to changing the crypto configuration type.

Note: The TKE Workstation is required for key management of the Crypto Express EP11 Coprocessors.

If you select **Accelerator**, you can zeroize the selected Crypto Express CCA Coprocessors by indicating **Zeroize the Coprocessor** on the Crypto Type Configuration window.

To select a crypto type configuration:

1. A power-on reset of the CPC must be complete.
2. Open the **Cryptographic Configuration** task in system programmer or service representative role.

   The Cryptographic Configuration window lists the Crypto Expres features installed on the CPC and provides controls for working with them.
3. Select from the list the Crypto Express features that you want to change the crypto type configuration.
4. Click **Crypto Type Configuration**.

   The Crypto Type Configuration window displays information on the selected Crypto Express features.
5. Select a configuration type for the Crypto Express features.
6. Zeroize the Crypto Express CCA Coprocessors when selecting an Crypto Express Accelerator crypto type.
7. Click **Apply** to change the crypto type configuration.

UDX configuration

Use the UDX Configuration to add customized operations to the selected Coprocessor installed on your system. The UDX configuration provides the capability to develop your own UDX Segment 3 image file and load your custom Segment 3 image file onto one or more Coprocessors. To view the Segment 3 details, click **View Details** on the Cryptographic Configuration window. The Segment 3 image file is built and loaded onto a removable media using a xSeries server workstation. For more information on building a UDX Segment 3 image file go to the following website at:

- Crypto cards (www.ibm.com/security/cryptocards)
- Click on Library on the navigation bar.

Note: The recognized file name for the UDX file that is signed is *.CCA.UDX.pk1

To configure for User Defined Extension (UDX):

1. The selected coprocessors must be installed, and the CPC must be power-on reset to activate the UDX configuration. Otherwise, to import a UDX file:
2. Open the **Cryptographic Configuration** task.

The Cryptographic Configuration window lists the coprocessors installed on the CPC and provides controls for working with them.

3. Select the Coprocessor to configure for UDX.
4. Click **UDX Configuration** to configure the coprocessor for UDX configuration.

   The UDX Configuration window displays detailed information for the coprocessor configured for UDX capability and provides controls for working with them.
5. Click **Import From Media** to import the UDX configuration file from the removable media to the Support Element hard drive.
6. Click **Import From FTP Server** to import a secure FTP location.
7. Click **Activate** to load the UDX configuration data to the selected Coprocessor.
8. Click **Reset to Default** to remove (deactivate) the UDX file from the crypto adapter.

Zeroize

This window cautions that you are about to clear the cryptographic keys from the selected Coprocessor(s) or Accelerator(s). Use the window's controls to confirm or cancel your request to zeroize the Coprocessor(s) or Accelerator(s).

Important: When **Zeroize** is selected on this window, you must re-enter the selected Coprocessor(s) or Accelerator(s) key data to re-enable cryptographic operations.

Zeroizing the selected Coprocessor(s) or Accelerator(s) clears the cryptographic keys from the Coprocessor(s) or Accelerator(s) hardware data by resetting it to binary zeros.

Note: The selected Coprocessor(s) or Accelerator(s) should be zeroized manually only when absolutely necessary, typically the Coprocessor(s) or Accelerator(s) must be cleared immediately.

- You must zeroize selected Coprocessor(s) or Accelerator(s) prior to transferring ownership of the Coprocessor(s) or Accelerator(s) hardware.
- In an emergency, you may want to zeroize selected Coprocessor(s) or Accelerator(s) to maintain the security of encrypted data.

Additional functions on this window include:

Zeroize
To only clear cryptographic keys from the cards specified, click **Zeroize**.

Cancel
To exit the current task, click **Cancel**.

Domain Management

This window allows you to clear the cryptographic keys within the given usage domain(s). When a crypto with the given associated usage domains are removed from a partition, this partition no longer has access to the cryptographic keys. If this crypto is assigned to a different partition utilizing the same usage domains as before, this new partition has access, possibly unintentional access, to the cryptographic keys. Therefore, when a crypto is removed from an active partition, the Usage Domain Zeroize window displays, providing the opportunity to clear the cryptographic keys within the given usage domain(s).

Cryptographic number
Displays the crypto number assigned to the selected crypto

Cryptographic status
Displays the current state for the selected crypto

Cryptographic type
Displays the Crypto Express feature type.

Usage domain index table

Usage domain index
Displays the number associated with the usage domain

Partition Name
Displays the partition name the crypto is in

Crypto State
Displays the cryptos current state in the partition

Compliance mode
Displays the current standard compliance of the cryptos. Compliance mode returns to default after zeroize of card, zeroize of domain, activation of UDX, and removal of UDX from Segment3.

CCA compliance levels
Non-compliant (default)

PCI-HSM 2016

PCI-HSM (migration)

EP11 compliance levels
FIPS 2021

FIPS 2024

Administrative FIPS 2021

FIPS 2009

BSI 2009

FIPS 2011

BSI 2011

BSI Common Criteria 2017

You can work with the tables by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears. The icons perform the following functions in the crypto table:

Select All
Selects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Deselect All
Deselects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header to change from ascending to descending order. Click **OK** when you have defined your preferred order.

Show Filter Row

Defines a filter for a table column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the check box next to the filter that you want in the filter row.

Clear All Filters

Returns to the complete table summary. The table summary includes the total number of items that pass the filter criteria and to the total number of items.

Clear All Sorts
Returns the table back to the default order.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Zeroize
To clear cryptographic keys within the given usage domain(s), click **Zeroize**.

Cancel
To exit the current task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Zeroize All

This window cautions that you are about to clear the cryptographic keys from all Coprocessors or Accelerators and delete the UDX file. Use the window's controls to confirm or cancel your request to clear the cryptographic keys from all Coprocessors or Accelerators.

Note: When **Zeroize All** is selected on this window, you must re-enter the Coprocessors or Accelerators key data to re-enable cryptographic operations.

Zeroizing All Coprocessors or Accelerators deletes the configuration data and clears the cryptographic keys for all Coprocessors or Accelerators by resetting it to binary zeroes. This includes clearing cryptographic secure keys, configuration data, and any other secure hardware data.

Note: The Coprocessors or Accelerators should be zeroized manually only when absolutely necessary, typically when coprocessor configuration data must be erased immediately. For example:

- You must clear the cryptographic keys for all Coprocessors or Accelerators prior to selling or transferring ownership of the Coprocessors or hardware.
- You may want to clear the cryptographic keys for all the Coprocessors or Accelerators to maintain the security of encrypted data.

Additional functions on this window include:

Zeroize All
To clear all cryptographic keys from the cards and delete configuration data from the system, click **Zeroize All**.

Cancel
o close the window without clearing cryptographic keys from all Coprocessors or Accelerators, click **Cancel**.

Cryptographic Details

This window displays detailed information about an installed Crypto Express feature.

Number
Displays the ID number assigned by the system to identify the Crypto Express features.

PCHID
Displays the Physical Channel Identifier (PCHID) assigned to the Crypto Express features.

Status
Indicates the status of the Crypto Express feature card; such as, operating, deconfigured, or installed.

Type
Indicates whether the Crypto Express cryptographic card is configured to operate as a CCA coprocessor, EP11 coprocessor, or an accelerator.

TKE commands
Indicates whether TKE commands are permitted or denied for the selected Crypto Express CCA Coprocessors.

Card location
Displays the physical location of the card in the frame.

Card serial number
Displays the serial number of the Crypto Express features plugged into the specified card location.

Crypto serial number
Displays the serial number of the crypto adapter contained in the Crypto Express features.

Crypto part number
Indicates the crypto part number for the crypto adapter contained in the Crypto Express features.

Secure module part number
Displays the module part number of the crypto adapter in the Crypto Express features.

FPGA version
Indicates the crypto Field Programmable Gate Array (FPGA) version for the crypto adapter contained in the Crypto Express features. The version is programmable and can be changed by firmware updates.

ASIC version
Indicates the crypto ASIC version for the selected Crypto Express features. The version is programmable and can be changed by firmware updates.

Card version
Indicates the crypto card version for the crypto adapter contained in the Crypto Express features. The card version is programmable and can be changed by firmware updates.

Number of concurrent internal code changes since last hardware reset
Displays the number of concurrent internal code changes for the selected Crypto Express feature since the last hardware reset.

Segment 1 image information

Segment 1 is an area of the selected Crypto Express feature that holds self-testing code (POST) which ensures the card is operating properly, and code that supports the secure update of firmware in Segments 1, 2, and 3.

Name
Displays the name that was specified when the image was built.

Hash Data
Uniquely identifies the image in Segment 1.

Segment 2 image information

Segment 2 is an area of the selected Crypto Express feature that holds the operating system for the card, as well as a small amount of self-testing code (POST) code which ensures the card is operating properly.

Name
Displays the name that was specified when the image was built.

Hash Data
Uniquely identifies the image in Segment 2.

Segment 3 image information

Segment 3 is an area of the Crypto Express feature that holds the Common Cryptographic Architecture (CCA) application code. This is also the area where a User-Defined Extension (UDX) image would reside, if a UDX Image was activated. If a UDX image is not activated, then the Default image resides in the Segment area. A UDX is a customized version of the CCA code containing specialized functions.

Operating Mode
Describes the type of image activated in the Segment 3, either UDX or the Default. If the selected Crypto Express features are deconfigured, the UDX status indicates *Not available*. This UDX image is imported from a USB flash memory drive or DVD using the UDX Configuration option.

Timestamp
Indicates the time stamp indicating when the UDX image or default image in Segment 3 was created.

Name
Displays the name that was specified when the image was built.

Hash Data
Uniquely identifies the image in Segment 3.

Additional functions on this window include:

Close
To close the window and return to the previous window, click **Close**.

Help
To display help for the current window, click **Help**.

TKE Commands Configuration

Use this window to indicate whether you want TKE commands permitted or denied for the selected Crypto Express CCA Coprocessors. The TKE workstation manages secure functions of the selected Crypto Express CCA Coprocessors only when permission is given. If permission is denied, all requests for information or commands to the selected Crypto Express CCA Coprocessors from the TKE workstation is denied.

Note: Permitting TKE access with the default TKE communication keys set can allow unauthorized access. For security reasons the user should immediately change the default value of the keys from the TKE.

Cryptographic number
Indicates the cryptographic number for the selected Crypto Express CCA Coprocessors to permit or deny TKE commands.

Status
Indicates the status of the selected Crypto Express CCA Coprocessors. (Operating, Deconfigured)

Type
Indicates the type of selected Crypto Express CCA Coprocessors.

TKE Commands
Indicates if the TKE commands are permitted or denied for the Crypto Express CCA Coprocessors.

You can work with the tables by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears. The icons perform the following functions in the crypto table:

Select All
Selects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Deselect All
Deselects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the

column header to change from ascending to descending order. Click **OK** when you have defined your preferred order.

Show Filter Row

Defines a filter for a table column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the check box next to the filter that you want in the filter row.

Clear All Filters

Returns to the complete table summary. The table summary includes the total number of items that pass the filter criteria and to the total number of items.

Clear All Sorts
Returns the table back to the default order.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Permit
To permit TKE commands, click **Permit**.

Deny
To deny TKE commands, click **Deny**.

Cancel
To close the window without changed the selected coprocessor current settings, click **Cancel**.

Help
To display help for the current window, click **Help**.

UDX Configuration

Use this window to import and activate a UDX for the selected Coprocessor installed on your system and to reset the Segment 3 area to the Default image. This window also indicates the imported Coprocessor UDX files on your system.

Note: The recognized file name for the UDX file that is signed: *.CCA.UDX.pk1

Use the **UDX Configuration** window to:

- **Import** a new UDX image from a removable media or FTP location
- **Delete** or zeroize a UDX image from the hard disk
- **Activate** the UDX image into Segment 3 area
- **Reset to Default** to remove (deactivate) the UDX file from the crypto adapter.

Select a Cryptographic Number, then select an action for the Segment 3 area.

Import or delete a UDX file

You can copy a UDX file to the Support Element hard drive hard drive from a removable media and use for subsequent UDX activation.

Import from FTP
To import the UDX file from a secure FTP location, click **Import from FTP**.

Import from Media
To import the UDX file from a removable media to store on the Support Element hard disk, click **Import from Media**.

Delete
To delete the UDX file from the Support Element hard disk, click **Delete**.

UDX Configuration table

The UDX configuration describes the Segment 3 area of the selected Coprocessor which holds the Common Cryptographic Architecture (CCA) application code. This window displays exactly what is located into Segment 3. You can find more detailed help on the following elements of this window:

Number
Displays a number assigned by the system to identify the selected coprocessor.

Type
Indicates if the selected Crypto Express features are operating as a coprocessor or accelerator.

Status
Displays the status of the selected coprocessor; such as, operating, deconfigured, or installed.

Image Activated
Indicates whether the UDX image is activated or the Default image is activated.

Image Timestamp
Displays the time stamp indicating when the UDX image or default image in Segment 3 was created.

Image Name
Displays the name that was specified when the image was built.

Pending Reset to Default
Displays the status if a reset to default is forced the next time the Coprocessor is operating online.

You can work with the tables by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears. The icons perform the following functions in the crypto table:

Select All
Selects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Deselect All
Deselects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header to change from ascending to descending order. Click **OK** when you have defined your preferred order.

Show Filter Row

Defines a filter for a table column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the check box next to the filter that you want in the filter row.

Clear All Filters

Returns to the complete table summary. The table summary includes the total number of items that pass the filter criteria and to the total number of items.

Clear All Sorts
Returns the table back to the default order.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Close
To close the window without changed the selected coprocessor current settings, click **Close**.

Help
To display help for the current window, click **Help**.

Import UDX from FTP

Use this window to import a UDX configuration file to a specified FTP destination. Use the **Protocol** field to select a secure network protocol for transferring files to the specified FTP destination.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

Additional functions on this window include:

Import
To import the UDX file from the specified secure FTP location , click **Import**.

Cancel
To close the window without performing the selected operation, click **Cancel**.

Help
To display help for the current window, click **Help**.

Crypto Type Configuration

This window displays what configuration type for the selected Crypto Express features currently operating on your system. The Crypto Express features must be deconfigured prior to changing the crypto configuration type.

Cryptographic Number
Displays the number assigned by the system to identify the Crypto Express feature.

Status
Displays the status of the Crypto Express; such as, operating, deconfigured, or installed.

Select a configuration for the Crypto

Specify the crypto configuration type for the Crypto Express features installed in your system. If changing from a CCA Coprocessor to an Accelerator, you can zeroize the cryptographic keys in the CCA Coprocessor when the crypto is operating online.

For a Crypto Express features select:

- CCA Coprocessor
- EP11 Coprocessor

  Note: The TKE Workstation is required for key management of the Crypto Express EP11 Coprocessor.
- Accelerator

You can work with the tables by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears. The icons perform the following functions in the crypto table:

Select All
Selects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Deselect All
Deselects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header to change from ascending to descending order. Click **OK** when you have defined your preferred order.

Show Filter Row

Defines a filter for a table column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the check box next to the filter that you want in the filter row.

Clear All Filters

Returns to the complete table summary. The table summary includes the total number of items that pass the filter criteria and to the total number of items.

Clear All Sorts
Returns the table back to the default order.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Apply
To perform the selected operation, click **Apply**.

Refresh
To update the displayed crypto type configuration information with the current configuration, click **Refresh**.

Cancel
To close the window without changing the crypto type configuration, click **Cancel**.

Help
To display help for the current window, click **Help**.

Cryptographic Management

Accessing the Cryptographic Management task

Use this task to release the cryptographic number from the card serial number that it is associated with. This is necessary because the cryptographic number assigned to that card continues to be associated with the adapter's serial number, unless the card is released, preventing reuse of the cryptographic number. Releasing the cryptographic number frees up the cryptographic number to be assigned to a new adapter serial number.

Each crypto adapter is assigned a crypto number of 0-n, where **n** is model dependent. This assignment is made when the card is installed in your system.

Use the Cryptographic Management window to view all:

- Installed cards with cryptographic number assignments
- Fenced cards that still maintain a cryptographic number assignment.

To release a cryptographic number from the adapter serial number:

Note: Depending on your user task role, you may only be able to view this task.

1. Open the **Cryptographic Management** task.

   The Cryptographic Management window list the cryptographic number assignments in the current system configuration.
2. Select the cryptographic number to be released from the adapter serial number list.
3. Click **Release**.

   The Cryptographic Management window confirms the cryptographic number you selected to be released.
4. Click **Confirm**.

   A message is displayed to indicate the release was successful.

Cryptographic Management

Use the **Cryptographic Management** task to release the cryptographic number from the card serial number that it is associated with. The Crypto Express (CCA Coprocessor, EP11 Coprocessor, and Accelerator) feature is a secure, integrated hardware that perform high-speed cryptographic functions. Each crypto adapter is assigned a cryptographic number (0-n), where **n** is model dependent, as part of the configuration process. This assignment is made when the card is installed in your system.

Note: Depending on your user task role, you may only be able to view this task.

Releasing the cryptographic number permits the cryptographic number to be assigned to a new card serial number. You should release the cryptographic number when a cryptographic feature is permanently removed from the system. The cryptographic feature must have a status of fenced before it can be released.

Use the Cryptographic Management window to view all:

- Installed cards with cryptographic number assignments
- Fenced cards that still maintain a cryptographic number assignment

To start the task to release a cryptographic number from the configuration, select a cryptographic number from the list box, then click **Release**.

Note: When you select a cryptographic number from the list box, all numbers associated with the card serial number are selected automatically.

Additional functions on this window include:

Release
To release the cryptographic number from the adapter serial number that it is associated with, click **Release**.

Cancel
To close the window without releasing the cryptographic number assigned to the cryptographic card, click **Cancel.**

Help
To display help for the current window, click **Help**.

Cryptographic Management List

Use this window to manage the release of the cryptographic numbers from the system configuration.

Number
The number assigned to the Crypto Express feature for identification purposes.

PCHID
The Physical Channel Path Identifier (PCHID) associated with the cryptographic number.

Card Location
The physical location of the cryptographic card in the frame.

Status
The status of the cryptographic card; installed, fenced, etc.

Card Serial Number
The serial number of the Crypto Express feature plugged into the specified card location.

Cryptographic Card Data

Use this window to review cryptographic card data.

Card Location
The physical location of the card in the frame.

Status
The status of the cryptographic card; installed, fenced, etc.

Card Serial Number
The serial number of the Crypto Express features plugged into the specified card location.

Type
Description of the type of cryptographic card for the Crypto Express feature.

Number
The number assigned to the Crypto Express feature for identification purposes.

PCHID
The Physical Channel Path Identifier (PCHID) associated with the cryptographic number.

Cryptographic Management Confirmation

Use this window to confirm the selected cryptographic numbers to be released from the system configuration.

You can find more detailed help on the following elements of this window:

Customer Information

Accessing the Customer Information task

Typically, if the service support system cannot determine the cause of the problem, it forwards the problem report and service request to a support center for further analysis by service personnel. The analysis may require a service representative to contact your company, preferably the person responsible for the system at the site where the system is located. So problem reports and service requests transmitted from the system's Support Element to the service support system also include such information.

You can use the Support Element workplace to customize information, referred to here as *account information*, that the system's service providers can use to contact your company and the person responsible for the system.

To customize account information:

1. Open the **Customer Information** task. The Customer Information window is displayed.
2. Select one of the following tabs from the Customer Information window:
   - Administrator
   - System
3. Enter the information in the fields provided.

   If the selected objects do not all have the same customer information, the information displayed on the Customer Information window will be information that applies to the first selected object. The information for the other objects will be displayed by tabs on the right.
4. Click **OK** to save the information and close the notebook.

Customer Information

Use this task to specify administrator, system, and account information about the system being installed. Completing these entry fields for each managed system allows your service structure to record necessary contact information.

Proceed through each tabbed page to specify the information for your administrator, system, and account fields.

Customer Information tabs

Provide the fields with contact information.

- Select **Administrator** to set up your administrator information for this system.
- Select **System** to set up information about this system.

Additional options are available with these pages:

OK
After providing the appropriate information in the fields, click **OK**.

Cancel
To exit this window without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Administrator

Use this page to specify the appropriate administrator information in the provided fields. This data is used to set up your customer contact information for this system.

Company name
Specify your company name in this required field, up to 36 characters.

Administrator name
Specify the name of an individual within the company to contact about the system in this required field, up to 36 characters.

Email address
Specify an email address of a company contact in this required field, up to 256 characters.

Phone number
Specify a telephone number for a company contact in this required field, up to 20 numeric characters.

Alternate phone number
Specify an alternate telephone number for a company contact, up to 20 numeric characters.

Street address
Specify the street address where the administrator resides in this required field. Include the building, floor, or room number, up to 68 characters for both address fields, combined.

Street address 2
Specify the second line of the street address where the administrator resides. Include the building, floor, or room number, up to 68 characters for both address fields, combined.

City or locality
Specify the city or locality where the administrator resides in this required field, up to 36 characters.

Country or region
Select the country or region where the administrator resides in this required field.

State or province
Select the state or province where the administrator resides in this required field.

Postal Code
Required to specify the postal or zip code where the administrator resides, up to 12 characters.

System

Use this page to specify the appropriate system information in the fields provided. This data is used to set up your customer account information for this system.

Use the administrator mailing address
Selecting this causes the administrator's mailing address to also be used as the system location.

Street address
Required to specify the street address where the system resides. Include the building, floor, or room number, up to 68 characters for both address fields, combined.

Street address 2
Specify the second line of the street address where the system resides. Include the building, floor, or room number, up to 68 characters for both address fields, combined.

City or locality
Specify the city or locality where the system resides in this required field, up to 36 characters.

Country or region
Select the country or region where the system resides in this required field.

State or province
Select the state or province where the system resides in this required field.

Postal code
Specify the postal or zip code where the system resides in this required field, up to 12 characters.

Customize API Settings

Accessing the Customize API Settings task

This task allows you to enable or disable an SNMP agent and set up a community name file and event notification information for an SNMP agent from the **SNMP** tab.

Note: If **Customizable Data Replication** is ***Enabled*** on this Hardware Management Console (using the **Configure Data Replication** task), the data the is specified in this task might change depending on automatic replication from other Hardware Management Consoles configured on your network. For more information about data replication, see **Configure Data Replication** task.

For more information on SNMP, see *SNMP Application Programming Interfaces*, SB10-7171.

You can allow other system management applications to use the Management Application Programming Interfaces (APIs) to the Support Element console application. Management APIs allow applications to exchange information about objects and send commands to an object managed by the Support Element console application. This task allows you to enable or disable an SNMP agent and set up a community name file and event notification information for an SNMP agent from the **SNMP** tab. For more information see *SNMP Application Programming Interfaces*, SB10-7171.

To customize API settings:

1. Open the **Customize API Settings** task. The Customize API Settings window is displayed.
2. From this window you can enable SNMP APIs and add, change, or delete community names, SNMPv3 users, and event notification information. You can also select to have a TLS encrypted connection.
3. Click **OK** to save the SNMP configuration and continue the configuration.

Customize API Settings

Use this task to customize the settings that support using Application Programming Interfaces (APIs) to the Support Element Application.

SNMP
Use this tab to enable and customize the SNMP settings.

Additional functions for this window include the following:

OK
To save the configuration, click **OK**.

Cancel
To exit this window and discard any changes made, click **Cancel**.

Help
To display help for the current window, click **Help**.

SNMP

Use this page to customize the settings that support using Management Application Programming Interfaces (APIs) to the Support Element Application.

You can find more detailed help on the following elements of this window:

Enable SNMP APIs

Enable
To allow other system management applications to use Management APIs to the Support Element Application, select **Enable**.

The Management APIs include:

Data exchange APIs
Allow applications to exchange information about objects managed by the console Application.

Command APIs
Allow applications to send commands to objects managed by the Support Element Application.

TLS Only
To use the TLS encrypted connection, select **TLS Only**.

Allow capacity change API requests
To allow for temporary capacity upgrades to be done through the automation process, select **Allow capacity change API requests**. The selection is used to indicate that automation requests to add or remove temporary capacity upgrades are allowed or not allowed.

SNMP agent parameters
Specify the parameters to use to start the Simple Network Management Protocol (SNMP) agent when the console Application starts.

Community Names

Specifies the community name(s) the Support Element Application must use to request SNMP information from the SNMP agent.

The Community Names table displays the following information:

Name
Specifies the community name used to verify that a request for SNMP information is valid when a manager makes an SNMP request.

Address
Specifies the IPv4 or IPv6 internet address.

Network Mask
Specifies a network mask that is logically ANDed with the IP address of the manager making an SNMP request.

Access Type
Specifies the access you want to allow SNMP requests.

The following options are available from this section of the window:

Add...
To add a new community names entry, click **Add...**.

Change...
To change the community name entry information for the selected entry, click **Change...**.

Delete
To delete the community name entry information for the selected entry, click **Delete**.

Community Name Information

Specify the community name the Support Element Application must use to request SNMP information from the SNMP agent.

A community name is similar to a password. It is used by an SNMP agent to validate requests for information received from system management applications.

The SNMP agent provides SNMP information to system applications authorized to manage another application and its objects.

Enabling Support Element Console Application Management APIs requires the support of an SNMP agent.

Note: The community name is case sensitive and cannot exceed 15 characters.

The community name you specify must match exactly the community name in the SNMP information for this console for its SNMP agent to validate and accept requests from the Support Element Application for SNMP information.

Name
This field contains the community name. Specify a unique string of characters (up to 15 characters), which is used to verify that a request for SNMP information is valid when a manager makes an SNMP request. The community name it is using must match the community names specified in this field. If it does not match, the SNMP request is not processed. The community name is similar to a password.

Address
Specify an IPv4 or IPv6 internet address (IP address).

The IPv4 address is written as four decimal numbers, representing the four bytes of the IP address, separated by periods (for example, `192.0.2.0`). The IPv6 address can be written as eight groups of four hexadecimal digits, separated by colons (for example, `2001:0db8:0000:0000:0202:b3ff:fe1e:8329`).

Note: For IPv6 simplification, you can eliminate leading zeros (for example, `2001:db8:0:0:202:b3ff:fe1e:8329`) or you can use a double colon in place of consecutive zeros (for example, `2001:db8::202:b3ff:fe1e:8329`).

When a manager makes an SNMP request, a logical AND is performed on its address and the value specified in the network mask field. If the result of the logical AND matches the value specified in the address field, the request is processed.

If you specify a specific IPv4 address in this field, only the host using that IP address can use the community name specified in the name field. Enter a network mask of 255.255.255.255 if you specify a specific IPv4 IP address in this field.

If you specify a specific IPv6 address in this field, only the host using that IP address can use the community name specified in the name field. Enter a network mask of 128 if you specify a specific IPv6 IP address in this field.

To allow any host with the correct community name to make SNMP requests:

- For IPV6, specify : : in the address field and 0 in the network mask field.
- For IPV4, specify 0.0.0.0 in the address field and 0 in the network mask.

Network mask / Prefix
This field contains a network mask that is logically ANDed with the IP address of the manager making an SNMP request. If the result of the logical AND is equal to the address specified in the address field and the community name matches, the request is processed.

To allow SNMP requests only from the host specified in the address entry field, specify a network mask of 255.255.255.255 for an IPv4 address or specify a network mask of 128 for an IPv6 address.

To allow any host with the correct community name to make SNMP requests:

- For IPV6, specify a network mask of 0 and an address of : :.
- For IPV4, specify a network mask of 0 and an address of 0.0.0.0.

Read only
If you want to allow SNMP requests with valid community names to have only read access to the SNMP agent information on this system, select **Read only**.

Read/write
If you want to allow SNMP requests with valid community names to have write access to the SNMP agent information on this system, select **Read/write**.

OK
To save the current settings in this window, click **OK**.

Cancel
To exit this window, discard any changes made, and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

SNMPv3 Users

Specifies the SNMPv3 user(s) the Support Element Application uses. SNMPv3 provides enhanced security via password based authentication and encryption.

The SNMPv3 Users table displays the following information:

User Name
Specifies the SNMPv3 user name.

Access Type
Specifies the access allowed to the SNMPv3 user.

The following options are available from this section of the window:

Add..
To add a new SNMPv3 user entry, click **Add...**.

Change...
To change the SNMPv3 user name information for the selected entry, click **Change...**.

Delete
To delete the selected SNMPv3 user entry, click **Delete**.

SNMPv3 User Information

Use this window to provide an SNMPv3 user name, password, and access type.

User Name
Specify an SNMPv3 user name. The user name must be at least 8 characters in length and cannot exceed 32.

Password
Specify a valid password for the SNMPv3 user. The password must be at least 8 characters in length and cannot exceed 32.

Read only
To allow only read access to the specified user name, select **Read only**.

Read/write
To allow read and write access to the specified user name, select **Read/write**.

OK
To save the current settings in this window, click **OK**.

Cancel
To exit this window, discard any changes made, and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Event Notification Information

This information controls the distribution of messages about events that affect objects managed by the Support Element Application.

The following options are available from this section of the window:

Add...
To add a new event notification information entry, click **Add...**.

Change...
To change the event notification entry information for the selected entry, click **Change...**.

Delete
To delete the selected event notification information entry, click **Delete**.

Event Notification Information

Use this window to add or change information that controls the distribution of trap messages about events that affect objects that are managed by the Support Element Application.

Trap messages are unsolicited notifications of significant system events that are sent by an SNMP agent to an SNMP client.

TCP/IP address
Specify the host name or IPv4 or IPv6 TCP/IP address of the location where you want SNMP trap messages sent when selected events occur.

The IPv4 address is written as four decimal numbers, representing the four bytes of the IP address, which is separated by periods (for example, `192.0.2.0`). The IPv6 address can be written as eight groups of four hexadecimal digits, which are separated by colons (for example, `2001:0db8:0000:0000:0202:b3ff:fe1e:8329`).

Note: For IPv6 simplification, you can eliminate leading zeros (for example, `2001:db8:0:0:202:b3ff:fe1e:8329`) or you can use a double colon in place of consecutive zeros (for example, `2001:db8::202:b3ff:fe1e:8329`).

Port number
Specify the TCP/IP port number when defining SNMP trap recipients, if it's something other than the default SNMP trap port of `162`.

Protocol
Select one of the following protocols:

TLS over TCP
To use TLS over TCP protocol, select **TLS over TCP**. This protocol also allows you to select **Allow self-signed or untrusted server certificates**. Use the **Certificate Management** task to import a certificate that you want to trust for this use.

UDP
To use the UDP protocol, select **UDP**.

TCP
To use the TCP protocol, select **TCP**.

Events table icons
You can use the table icons or **Select Action** from the table toolbar to perform the following functions on the Events table:

Select All
To select all the events, click **Select All**.

Deselect All
To deselect all the events, click **Deselect All**.

Edit Sort
Performs multi column sorts of the events in the table in ascending or descending order.

Clear All Sorts
Returns to the default ordering.

Events table
Select one or more events for which trap messages are sent to the specified location. The events affect objects that are managed by the Support Element Application.

Activation Profile Change
To send a message when the activation profile for an object has changed, select **Activation Profile Change**.

Capacity Change
To send a message when a hardware object's temporary capacity has changed, select **Capacity Change**.

Capacity Record Change
To send a message when a temporary capacity record for a hardware object has changed, select **Capacity Record Change**.

Console Application Ended
To send a message when the Support Element Application ends, select **Console Application Ended**.

Console Application Started
To send a message when the Support Element Application starts, select **Console Application Started**.

Disabled Wait
To send a message when an operating system object enters a disabled wait, select **Disabled Wait**.

Exception State
To send a message when the status of an object changes from an acceptable status to an unacceptable status, or from an unacceptable status to an acceptable status, select **Exception State**.

Exclude Refresh Messages
To disable the sending of a message when an object receives a refresh message, select **Exclude Refresh Messages**.

Hardware Message Deletion
To send a message when a message for a hardware object is deleted, select **Hardware Message Deletion**.

Hardware Messages
To send a message when a hardware object receives a new or refresh message, select **Hardware Messages**.

Log Events
To send a message when a log event occurs on an object, select **Log events**.

Messages
To send a message when a Hardware Message or Operating System Message occurs on an object, select **Messages**.

Name Change
To send a message when the name of an object changes, select **Name Change**.

Object Creation
To send a message when an object definition is added, select **Object Creation**.

Object Destruction
To send a message when an object definition is removed, select **Object Destruction**.

Operating System Messages
To send a message when an operating system object receives a new or refresh message, select **Operating System Messages**.

Security Events
To send a message when a security event occurs for an object (such as logons or object definitions), select **Security Events**.

Shutdown
To send a message when a shutdown occurs, select **Shutdown**.

Status Change
To send a message when the status of an object changes, select **Status Change**.

OK
To save the current settings in this window, click **OK**.

Cancel
To exit this window, discard any changes that are made, and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Customize Console Services

Accessing the Customize Console Services task

This task enables or disables Support Element services. A Support Element service is a facility or function of the Support Element Console Application that allows the console to interact with other consoles and systems. Enabling a service lets the console provide tasks and perform operations associated with the service. Disabling a service prevents the console from providing tasks and performing operations associated with the service.

Services include:

Remote power off or restart
Controls whether this Support Element can be powered off or restarted by a user accessing it from a remote workstation. If this service is Disabled, only local users at this Support Element can use the **Power Off or Restart** task. Only user IDs with system programmer or service roles can access this option.

Automatic SE Switchover
Controls whether the Support Element is to be automatically switched to the alternate Support Element.

Console messenger
Controls whether the console messenger facility is active on this Support Element or not. The console messenger facility allows users of this Support Element to send and receive instant messages and broadcast messages to other users of this console and remote consoles.

Network message forwarding

You can use the Support Element workplace to control whether the Support Element console will serve as a network message relay node or not. If the Support Element console is configured to act as a relay, it will provide inter-console forwarding of network messages used by forwarding-enabled Support Element consoles; services, such as console messenger service. This forwarding can allow these forwarding-enabled services to communicate between console nodes that do not have direct network connectivity with each other.

Large retrieves from the support system
Controls whether this Support Element can retrieve internal code changes from the support system for engineering change streams that are expected to contain a large amount of data.

Check held LIC changes during install
Controls whether this console will check the support system for any LIC changes on hold when an install and activate is performed. *Enabled* is the recommended setting in order to prevent activation of released fixes that have later been discovered to have problems.

Licensed Internal Code security mode
Controls whether to change the Licensed Internal Code security mode to monitor the integrity and security protected firmware file on the Support Element.

Minimum TLS version
Determines the minimum Transport Layer Security (TLS) version that the console will negotiate. The default is set at **TLSv1.2**. **TLSv1.3** is ***not*** the recommended selection.

Transmit system availability data
Sends system availability data to the support system for analysis.

To enable or disable Support Element services:

1. Open the **Customize Console Services** task. The Customize Console Services window is displayed.
2. Select **Enabled** or **Disabled** for each service.
3. Click **OK** to complete the task.

Customize Console Services

Use this window to enable or disable console services.

A *console service* is a facility or function of the Support Element Console Application that allows the console to interact with other consoles and systems.

The window displays a list of the services for each console service. The controls next to the services initially indicate whether the console services are currently enabled or disabled. You can use the controls, if necessary, to change the settings of the services:

- *Enabling* a service allows the console to provide tasks and perform operations that are associated with the service.

- *Disabling* a service prevents the console from providing tasks and performing operations that are associated with the service.

Remote power off or restart

Use this service to control whether this Support Element can be powered off or restarted by a user accessing it from a remote workstation. If this service is **Disabled**, only local users at this console can use the **Power Off or Restart** task. Only user IDs with system programmer or service roles can access this option.

Note: This option cannot be enabled from a remote Hardware Management Console.

Disabled
Prevents the power off or restart of this console by a remote user.

Restart console
Allows the restart of this console by a remote user.

Power off and restart
Allows the power off and restart of this console by a remote user.

Change...
To enable or disable remote restart or power off of this console, click Change....

Automatic SE switchover

Use this service to control whether the Support Element is to be automatically switched from the Support Element to the alternate Support Element.

Enabled
To allow the switch from Support Element to alternate Support Element, select **Enabled**.

Disabled
To prevent the switch from Support Element to alternate Support Element, select **Disabled**.

Console messenger

Use this service to control whether the console messenger facility is active on this console or not.
The console messenger facility allows users of this console to send and receive instant messages and broadcast messages to other users of this console and remote consoles.

Enabled
To allow users on this console to send and receive instant messages and broadcast messages select **Enabled**.

Disabled
To prevent users on this console from sending or receiving instant messages and broadcast messages select **Disabled**.

Network message forwarding

Use this service to control whether this console serves as a network message relay node or not. If the console is configured to act as a relay, it provides inter-console forwarding of network messages that are used by forwarding-enabled console services, such as the console messenger service. This forwarding can allow these forwarding-enabled services to communicate between console nodes that do not have direct network connectivity with each other.

Enabled
To allow this console to act as a network message relay node and forward network messages to other consoles to which it is connected select **Enabled**.

Disabled
To prevent this console from forwarding network messages select **Disabled**.

Large retrieves from support system

Use this service to control whether this console can retrieve internal code changes from the support system for Engineering Change (EC) streams that are expected to contain a large amount of data.

Enabled
To authorize this console to retrieve all available internal code changes from the support system when there is a broadband connection, select **Enabled**.

Disabled
To exempt this console from retrieving from the support system for EC steams that are expected to contain a large amount of data, select **Disabled**. Internal code changes for the exempted EC streams will need to be retrieved from media.

Check held LIC changes during install

Use this service to control whether this console will check the support system for any LIC changes on hold when an install and activate is performed.

Note: *Enabled* is the recommended setting in order to prevent activation of released fixes that have later been discovered to have problems.

Enabled
To authorize this console to check the support system for any LIC changes on hold when an install and activate is performed, select **Enabled**.

Disabled
To exempt this console from checking the support system for any LIC changes on hold when an install and activate is performed, select **Disabled**.

Licensed Internal Code security mode:

Use this service to change the Licensed Internal Code security mode on the console.

Change...
To change the Licensed Internal Code security mode, click Change....

Minimum TLS version

Use this service to determine the minimum Transport Layer Security (TLS) version that the console negotiates. The default is set at **TLSv1.2**. **TLSv1.3** is ***not*** the recommended selection.

Transmit system availability data

Use this service to send system availability data to the support system for analysis.

Enabled
Specifies that this console allows the transmission of system availability data.

Disabled
Specifies that this console does not allow transmission of system availability data.

Change...
To enable or disable transmission of system availability data or to change the transmission schedules, click Change....

Additional functions are available from this window:

OK
After you have changed the settings of the services, click **OK**.

Cancel
To end this task without changing any settings, click **Cancel**.

Help
To display help for the current window, click **Help**.

Change Remote Power Off and Restart Settings

Use this window to control whether this primary Support Element can be remotely powered off and restarted. Only user IDs with system programmer or service roles can access this option.

Disabled
To not allow remote power off or restart for this SE, select **Disabled**.

Restart
To allow this SE to be restarted remotely, select **Restart**.

Power off and restart
To allow this SE to be powered off and restarted remotely, select **Power off and restart**.

Additional functions are available from this window:

OK
After you have changed the settings, click **OK**.

Cancel
To end this task without changing any settings, click **Cancel**.

Help
To display help for the current window, click **Help**.

Change Licensed Internal Code Security Mode

Use this window to change the Licensed Internal Code security mode for monitoring the integrity and security of protected firmware files on the Support Element.

The ACSADMIN default user or a user that has permission to the **Change Licensed Internal Code Security Mode** task can change **Monitor Mode** to **Monitor and Protect Mode**. The SERVICE default user or user that has the Service Representative tasks role or a role based on the Service Representative tasks role can change **Monitor Mode** to **Monitor and Protect Mode** and **Monitor and Protect Mode** to **Monitor Mode**. When changing from **Monitor and Protect Mode** to **Monitor Mode**, you must be physically present at the Primary Support Element and Alternate Support Element to confirm the console changes when rebooted. Physical presence is not required when changing from **Monitor Mode** to **Monitor and Protect Mode**.

Note: This confirmation is required on both the primary and alternate Support Elements.

The Support Element complies with the National Institute of Standards and Technology (NIST) BIOS protection guidelines for servers SP 800-147B.

Monitor Mode
To provide threat detection, reporting, and analysis, select **Monitor Mode**. If a potential threat is detected, a hardware message is generated. Additionally, the next level of support will be required to reload the Support Element.

Monitor and Protect Mode
To provide threat detection, reporting, analysis, and stop all operations when a threat is detected, select **Monitor and Protect Mode**. If a potential threat is detected, a hardware message is generated and the console is stopped. Additionally, the next level of support will be required to reload and restart the Support Element.

Additional functions are available from this window:

OK
After you have changed the settings of the services, click **OK**.

Cancel
To end this task without changing any settings, click **Cancel**.

Help
To display help for the current window, click **Help**.

Manage system availability collection

Use this window to control the transmission of system availability data to system support for analysis. See **GUIDANCE** for more information.

Enable system availability analysis
To allow the transmission of system availability data, select **Enable system availability analysis**.

Health and diagnostic data

Use this section to set up a weekly schedule for sending health and diagnostic data for analysis by service support or you can send it immediately.

Set weekly schedule
To set up a specific schedule each week to send the data, make a selection from the drop-down arrows for the day of the week and time of the day the data is sent for analysis.

Send data now
To send the health and diagnostic data for analysis immediately, click **Send data now**.

Active health data

Use this section to set up a daily schedule for sending active health data for analysis by service support or you can send it immediately.

Set daily schedule
To set up a specific schedule each day to send the data, make a selection from the drop-down arrow for the time of the day the data is sent for analysis.

Send data now
To send the active health data immediately, click **Send data now**.

More functions are available from this window:

Cancel
To return to the previous window without making changes, click **Cancel**.

Apply
To save the settings, click **Apply**.

Help
To display help for the current window, click **Help**.

Customize Network Settings

Accessing the Customize Network Settings task

This task allows you to view the current network information for the Support Element console and to change the network settings as shown in the following list.

Identification
Contains the host name and domain name of the Support Element console.

Console name
Your Support Element console user name, the name that identifies your console to other consoles on the network. This console name is the short host name, for example:

```
seibm1
```

Domain name
An alphabetic name that Domain Name Services (DNS) can convert to the IP address. For example, DNS might convert the domain name 222.example.com to 192.0.2.0. The long host name consists of console name plus a period plus a domain name, for example:

```
seibm1.example.com
```

Netid
Displays the SNA network name of the network, which the system is attached through. Change this setting only when the network's SNA network name is changed or when the system is connected to a different network.

Console description
This description is for your use only. An example might be:

```
Main Support Element Console for customer finance
```

LAN Adapters
A summarized list of all (visible) Local Area Network (LAN) adapters. You can select any of the LAN adapters and click **Details...** to open a window allowing you to work with the basic LAN settings.

Name Services
The Domain Name Services (DNS) and domain suffix values.

Routing
Routing information and default gateway information.

The **Gateway address** is the route to all networks. The default gateway address (if defined) informs the Support Element console where to send data if the target station does not reside on the same subnet as this Support Element console. This information is needed to allow the Support Element console to connect to the support system by using the internet.

You can assign a specific LAN to be the **Gateway device** or you can choose "any."

You can select **Enable 'routed'** to start the routed daemon. (**Note:** Use this option only if a Routing Information Protocol (RIP) daemon is required.

STP/ETS Networks
Allows you to configure the Server Time Protocol/External Time Source (STP/ETS) network settings on the Support Element.

To customize the network settings:

1. Open the **Customize Network Settings** task. The Customize Network Settings window is displayed.
2. Proceed through the tabs and provide the appropriate information.
3. Click **OK** to save the changes and exit the task.

Note: Depending on the type of change that you make, the network or console automatically restarts or the console automatically reboots.

Customize Network Settings

Use this task to view the current network information for the Support Element and to make changes to those settings. From this window, you can view or change information pertaining to each of the following tabs.

- Identification
- LAN Adapters
- Name Services
- Routing
- “STP/ETS Networks” on page 462

Note: Depending on the type of change that you make, the network or console automatically restarts or the console automatically reboots.

OK
To save all changes made to the network configuration and exit this task, click **OK**.

Cancel
To exit this task without saving your changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Network Settings tabs

Click a tab to configure the network settings for your console.

Identification
Specify your console name, domain name, and console description to identify your console to the network.

LAN Adapters
Specify the LAN adapter for LAN adapter-specific information.

Name Services
Specify the DNS for configuring the console network settings.

Routing
Specify Routing information for configuring static routing options for the Support Element.

"STP/ETS Networks" on page 462
Configure the STP/ETS network settings on the Support Element.

Identification

Use this page to identify your console.

Specify the console name and the domain name to create the host name, sometimes known as the host name and the domain name suffix. It is important that you specify the correct domain name. If you do not know or are not sure, contact your system administrator.

Specify a console description you can use for your own reference.

Console name
Specify the name or identifier specified as your console name to identify your console on the network.

The console name cannot exceed eight characters. The characters can consist of:

- Uppercase letters (A - Z)
- Lowercase letters (a - z)
- Numerals (0 - 9)

Note: There are no restrictions on the first character for the console name.

The console name identifies your console to other consoles on the network. If you use a name other than your Support Element user name, you will not be properly identified on the network.

If you do not know or are unsure of your console name, contact your system administrator.

Domain name
Specify the name assigned as the domain name for your console.

This unique name identifies an Internet site.

If you do not know or are not sure of your domain name, contact your system administrator.

Netid
Displays the SNA network name of the network which the system is attached through the Support Element.

Change this setting only when the network's SNA network name is changed or when the system is connected to a different network. In either case, specify the new SNA network name in the field.

Console description
Specify a description for your Support Element that you want to use for reference and identification.

This description identifies your console in more detail. For example, your console name can be **HMC12** and your description can be **Main HMC for customer finance**.

LAN Adapters

Use this page to select a Local Area Network (LAN) adapter for adapter-specific information on that LAN adapter.

Select one adapter at a time in the list and click **Details...**.

LAN Adapters
Displays a list of LAN adapters to choose from to view and change the current settings.

Details...
To view and change current settings for the selected LAN adapter, click **Details...**.

LAN Adapter

Use this page to view and change current Local Area Network (LAN) adapter settings for your console.

LAN interface address
This consists of the Media Access Control (MAC) address on the card, the type of card (Token Ring or Ethernet), and the adapter name (for example, eth0, tr1). These values uniquely identify the LAN adapter and cannot be changed.

Media Speed
Specifies the speed in duplex mode of an ethernet adapter. Use the down arrow and select **Autodetection** unless you have a requirement to specify a fixed media speed.

Use IPv4 Address
Select this check box to allow entering IPv4 TCP/IP addresses for your systems network settings.

Primary TCP/IP address
Specify the TCP/IP address of the primary Support Element.

The TCP/IP interface address is the setting used to identify the Support Element while using Transmission Control Protocol/Internet Protocol (TCP/IP) for communications in the network. The TCP/IP interface address displays the TCP/IP address of the LAN interface.

The Support Element network settings are customized for the network it is connected to when it is installed. After that, there is no need to change the network settings while the configuration of the network remains unchanged. Only consider changing the network settings when:

- The Support Element remains connected to the same network, but a network address or identifier changes.
- The Support Element remains connected to the same network, but the console is no longer uniquely identified in the network due to the connection of additional devices to the network.
- The Support Element is connected to a different network.

Alternate TCP/IP address
Specify the TCP/IP address of the alternate Support Element.

The TCP/IP interface address is the setting used to identify the Support Element while using Transmission Control Protocol/Internet Protocol (TCP/IP) for communications in the network. The TCP/IP interface address displays the TCP/IP address of the LAN interface.

The Support Element network settings are customized for the network it is connected to when it is installed. After that, there is not need to change the network settings while the configuration of the network remains unchanged. Only consider changing the network settings when:

- The Support Element remains connected to the same network, but a network address or identifier changes.
- The Support Element remains connected to the same network, but the console is no longer uniquely identified in the network due to the connection of additional devices to the network.
- The Support Element is connected to a different network.

TCP/IP interface network mask
Specify the TCP/IP interface network mask of the Support Element adapter.

The TCP/IP network mask, combined with the TCP/IP address, identifies the subnetwork in which the HMC adapter is located.

LAN Adapter Details

Use this window to view and change the current settings for the selected LAN adapter.

- IPv6 Settings tab - Specify the IPv6 settings for your console.
- LAN Adapter tab - Specify the LAN adapter settings for your console.

OK
To save all changes and close this window, click **OK**.

Cancel
To close this window without saving your changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

IPv6 Settings

Use this page for allowing IPv6 configuration settings for the selected network adapter defined on this Support Element.

Autoconfigure IP addresses
To automatically configure IP addresses, select **Autoconfigure IP addresses** (a check mark appears).

If this option is selected, the autoconfiguration process includes creating a link-local address and verifying its uniqueness on a link, determining what information should be autoconfigured (addresses, other information, or both). In the case of addresses, whether they should be obtained through the stateless mechanism, the stateful mechanism, or both.

Autoconfigured Addresses table
This table lists the automatically configured IPv6 addresses for this adapter.

Static IP Addresses table
This table lists the statically configured IPv6 addresses for this adapter. Addresses can be added or selectively changed or removed from this table.

Add...
To add a valid IPv6 address for this adapter, click **Add...**.

Edit...
To change a selected IPv6 address, click **Edit...**.

Remove
To remove a selected IPv6 address, click **Remove**.

IPv6 Settings

Use this window to add a static IPv6 address.

IPv6 address
Specify a 128 bit IPv6 address.

IPv6 addresses are written as eight groups of four hexadecimal digits. For example, fe80:0:0:0:204:acff:feab:b811 is a valid IPv6 address. If one or more four digit groups are 0000, the zeros can be omitted and replaced with two colons (::).

Alternate Address
Specify a 128 bit IPv6 address for the alternate Support Element.

Prefix length
Specify a prefix length value.

The prefix length value is a decimal value that indicates the number of contiguous, higher-order bits of the address that make up the network portion of the address.

OK
To save all changes and close this window, click **OK**.

Cancel
To close this window without saving your changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Name Services

Use this page to specify Domain Name Services (DNS) for configuring the console network settings.

DNS is a distributed database system for managing host names and their associated Internet Protocol (IP) addresses. Using DNS means that people can use names, such as "www.example.com" to locate a host, rather than using the IP address (xxx.xxx.xxx.xxx). A single server may only be responsible for knowing the host names and IP addresses for a small subset of a zone, but DNS servers can work together to map all Domain names to their IP addresses. DNS servers working together allow computers to communicate across the Internet.

DNS enabled
To enable the Domain Name Services (DNS), select **DNS enabled** (a check mark appears). You may want to enable DNS because you have DNS servers for mapping IP addresses to host names.

To disable the DNS, deselect **DNS enabled**.

DNS Server Search Order
Displays the order in which the DNS server search is performed.

Add
To add the IP address to the list of configured DNS servers, click **Add**. The New DNS Server window is displayed. The following functions are available from this window:

DNS Server Address
Specify an IP address of the DNS server to be searched for mapping the host names and IP addresses in the **DNS Server Address** input area.

OK
To add the new DNS server address to the DNS Server Search Order list, click **OK**.

Cancel
To return to the previous window without adding a new DNS server address, click **Cancel**.

Help
To display help for the current window, click **Help**.

Remove
To delete a selected IP address from the list, click **Remove**.

Move Up
To move a selected IP address up in the list, click **Move Up**.

Move Down
To move a selected IP address down in the list, click **Move Up**.

Note: The DNS Server Search Order list is available only when the **DNS enabled** check box is selected.

Domain Suffix Search Order
Displays the order in which a domain suffix search is performed.

Add
To add a domain suffix to the list, click **Add**. The New Domain Suffix window is displayed. The following functions are available from this window:

Domain Suffix
Specify a domain suffix in the **Domain Suffix** input area.

OK
To add the new domain suffix to the Domain Suffix Search Order list, click **OK**.

Cancel
To return to the previous window without adding a new domain suffix, click **Cancel**.

Help
To display help for the current window, click **Help**.

Remove
To delete a selected domain suffix from the list, click **Remove**.

Move Up
To move a selected domain suffix up in the list, click **Move Up**.

Move Down
To move a selected domain suffix down in the list, click **Move Up**.

Note: The DNS Suffix Search Order list is available only when the **DNS enabled** check box is selected.

Note: If you do not know or are not sure of the IP address or the domain suffix of the DNS servers, consult your network administrator.

Routing

Use this page to specify routing information for configuring the console network settings. You can add, delete, or change routing entries and specify routing options for the Support Element.

Routing Information

This displays the Support Element's current static routing information. Click **New...** to add a new routing entry, **Change...** to edit the selected routing entry, or **Delete** to remove selected routing entries and specify routing options for the Support Element.

The routing information table displays:

Type

Net

Specifies a network-specific route. With a net route, the destination address is the TCP/IP address of a particular network. All TCP/IP communications destined for that network are routed using the TCP/IP address of the router, unless a host route also applies for the communication to the destination host address. When a conflict occurs between a host and net route, the host route is used.

Host

Specifies a host-specific destination. With a host route, the destination address is the TCP/IP address of a particular host. All TCP/IP communications destined for that host are routed through the router using the router address as the TCP/IP address.

Destination
Displays the TCP/IP address of the destination host, network, or subnet.

Gateway
Displays the TCP/IP address of the next hop in the path to the destination.

Subnet Mask
Displays the subnet mask used by network interfaces to add routes.

Interface
Displays the name of the network interface that is associated with the table entry.

Default Gateway Information

Gateway address
Displays the current gateway address. To change this default information, specify a new gateway address.

Note: The default gateway is the route to all networks. The default gateway address informs each personal computer or other network device where to send data if the target station does not reside on the same subnet as the source. If your machine can reach all stations on the same subnet (usually a building or a sector within a building), but cannot communicate outside the area, it is usually because of an incorrectly configured default gateway.

Gateway device
Displays the current gateway device. To change this default information, use the down arrow to choose a Gateway device.

Enable 'routed'
To enable the network routing daemon, select **Enable 'routed'**.

Note: Use this option only if a Routing Information Protocol (RIP) daemon is required. If you are not sure if this daemon is required, consult your network administrator.

- If a check appears this enables the routing daemon, 'routed'.
- If no check appears (to disable) this stops it from running and prevents any routing information from being exported from this Support Element.

Route Entry

Use this window to manage static routing information.

Route Type
Select a Route type:

Net
Specifies that a network is the target for this route. With net route, the destination address is the TCP/IP address of a particular network. All TCP/IP communications destined for that network are routed through the router using the TCP/IP address of the route, unless a host route also applies for the communication to the destination host address. When a conflict between a host and net route occurs, the host route is used.

Host
Specifies that a host is the target for this route. With a host route, the destination address is the TCP/IP address of a particular host. All TCP/IP communications destined for that host are routed through the router using the router address as the TCP/IP address.

Destination
Specify the TCP/IP destination network host or subnet address.

Gateway
Specify the TCP/IP gateway address for routing the IP packets. This must be in 32-bit dotted-decimal notation.

Subnet mask
Specify the subnet mask to use as the network mask when adding a route. This is the subnet work address for the host portion of the IP address. Network interfaces can use different subnet masks, providing the capability of adding routes by specifying a subnet mask (variable subnet routes). You must specify a subnet mask when adding a route, in 32-bit dotted-decimal notation.

Adapter
Select the adapter by using the down arrow. This is the name of the network adapter that is associated with the table entry.

OK
To save all changes and close this window, click **OK**.

Cancel
To close this window without saving your changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

STP/ETS Networks

Use this window to configure the Server Time Protocol/External Time Source (STP/ETS) network settings on the Support Element.

STP/ETS LAN Adapters

A list of STP/ETS LAN adapters is listed. Select an adapter and click **Details** for more information. The "STP/ETS Adapter Details" on page 463 window is displayed.

Select the **Active** checkbox to activate the IP address configuration for each STP/ETS LAN Adapter.

Note: Both adapters can be configured using the same IP subnet, but only a single adapter may be active on a particular subnet at any given time.

STP/ETS Routing Information

All routes are listed including **Network**, **Host**, and **Default** routes. You can select a route if it needs to be updated or deleted. You can also add a new route. The current Destination Address, Subnet Mask, Gateway Address, and Adapter Name are displayed.

Routes
Displays the routes that are available.

New
To add a route, click **New...**. The "STP/ETS Route Entry" on page 464 window is displayed.

Details
To view adapter details on a selected route, click **Details...**. The "STP/ETS Adapter Details" on page 463 window is displayed.

Note: The gateway address for a particular route tells ETS where to send data when a target is part of the destination subnet. This includes default routes which handle all targets not already defined by the local subnet or network/host routes. If your machine can reach all stations on the same subnet (usually a building or a sector within a building), but cannot communicate outside the area, it is usually because of incorrectly configured routes.

Delete
To remove a selected route from the list, click **Delete**.

STP/ETS Name Services Information

Use these tables to specify the STP/ETS Domain Name Services (DNS) information.

DNS Server Search Order
Displays the order in which the DNS server search is performed.

Add
To add the IP address to the list of configured DNS servers, click **Add**. The New DNS Server window is displayed. The following functions are available from this window:

DNS Server Address
Specify an IP address of the DNS server to be searched for mapping the host names and IP addresses in the **DNS Server Address** input area.

Remove
To delete a selected IP address from the list, click **Remove**.

Domain Suffix Search Order
Displays the order in which a domain suffix search is performed.

Add
To add a domain suffix to the list, click **Add**. The New Domain Suffix window is displayed. The following functions are available from this window:

Domain Suffix
Specify a domain suffix in the **Domain Suffix** input area.

Remove
To delete a selected domain suffix from the list, click **Remove**.

Additional functions on this window include:

OK
To add the new domain suffix to the Domain Suffix Search Order list, click **OK**.

Cancel
To return to the previous window without adding a new domain suffix, click **Cancel**.

Help
To display help for the current window, click **Help**.

STP/ETS Adapter Details

Use this window to view the details of the STP/ETS LAN adapters.

- "STP/ETS Adapter tab" on page 463
- "STP/ETS IPv6 Settings tab" on page 463

STP/ETS Adapter tab

Use this window to view and change the current settings for the selected STP/ETS LAN adapter.

Active
Select the **Active** checkbox to activate the IP address configuration for the STP/ETS LAN Adapter.

Note: Both adapters can be configured using the same IP subnet, but only a single adapter may be active on a particular subnet at any given time.

Local Area Network Information
Displays the interface name of the STP/ETS LAN adapter.

IPv4 Settings

Address
Provide a TCP/IP address.

Network Mask
Provide a TCP/IP interface network mask.

STP/ETS IPv6 Settings tab

Use this page to automatically configure IP addresses and provide a static IPv6 address.

Autoconfig Options

Autoconfigure IP addresses
To automatically configure IP addresses, select **Autoconfigure IP addresses** (a check mark appears).

If this option is selected, the autoconfiguration process includes creating a link-local address and verifying its uniqueness on a link, determining what information should be autoconfigured (addresses, other information, or both). In the case of addresses, whether they should be obtained through the stateless mechanism, the stateful mechanism, or both.

Autoconfigured STP/ETS IPv6 Addresses table
This table lists the automatically configured STP/ETS IPv6 addresses for this adapter.

IP Address
Displays a 128 bit IPv6 address.

Prefix Length
Displays a prefix length value.

Static IPv6 Address
Specify a static IPv6 address and prefix length.

IPv6 address
Provide an IPv6 address.

IPv6 addresses are written as eight groups of four hexadecimal digits. For example, fe80:0:0:0:204:acff:feab:b811 is a valid IPv6 address. If one or more four digit groups are 0000, the zeros can be omitted and replaced with two colons (::).

Prefix length
Provide a prefix length.

The prefix length value is a decimal value that indicates the number of contiguous, higher-order bits of the address that make up the network portion of the address.

OK
To save all changes and close this window, click **OK**.

Cancel
To close this window without saving your changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

STP/ETS Route Entry

Use this window to add or change an STP/ETS route.

Route Type
Three types of routes can be defined.

1. **Network route:** A route to a destination of any size. Required Information: *Destination Address, Subnet Mask, Gateway Address*
2. **Host route:** A route to a single address. Required Information: *Destination Address, Gateway Address*
3. **Default route:** The route to anything not already defined, either through a directly attached lan or through a network or host route. Required Information:*Gateway Address*

Destination
Specify the TCP/IP destination network host or subnet address.

Subnet mask
Specify the subnet mask to use as the network mask when adding a route. This is the subnet work address for the host portion of the IP address. Network interfaces can use different subnet masks, providing the capability of adding routes by specifying a subnet mask (variable subnet routes). You must specify a subnet mask when adding a route, in 32-bit dotted decimal notation.

Gateway
Specify the TCP/IP gateway address for routing the IP packets. This must be in 32-bit dotted decimal notation.

Adapter
Select the adapter by using the drop-down arrow. This is the name of the network adapter that is associated with the table entry.

OK
To save all changes and close this window, click **OK**.

Cancel
To close this window without saving your changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Customize Product Engineering Access

Accessing the Customize Product Engineering Access task

This task, used by an access administrator or a user ID that is assigned access administrator roles, enables or disables the authorization of Product Engineering access to the Support Element console. Once product engineering is enabled to access the Support Element console you can decide whether or not product engineering can access the system remotely.

With access authority and a specified time frame, Product Engineering can log on the Support Element console with an exclusive user identification that provides tasks and operations for problem determination.

Product Engineering access is provided by a reserved password and permanent user identification. You cannot view, discard, or change the password and user identification, but you can control their use for accessing the Support Element console.

To customize product engineering access:

1. Open the **Customize Product Engineering Access** task. The Customize Product Engineering Access window is displayed.
2. Select the appropriate accesses for product engineering or remote product engineering.
3. Click **OK** to save the changes and exit the task.

Customize Product Engineering Access

Use this window to set the authorization and a length of time for Product Engineering (PE) access to the console. When you enable Product Engineering access, you can also decide whether or not to allow Product Engineering to remotely access the console.

When access is authorized, a product engineer can use an exclusive user ID and reserved password to log on to the console that provides tasks for problem determination.

You cannot view, discard, or change the password and user identification, but you can control its use for logging on to the application by customizing the console's PE access setting.

Note: Although PE access does not compromise the security of your system or the console, this task completes your control of user access to them.

Product Engineering Access

Disable product engineering access
To prevent logging on the application with an exclusive user ID reserved for Product Engineering, select **Disable product engineering access**.

Enable product engineering access
To allow logging on the console with an exclusive user ID reserved for Product Engineering, select **Enable product engineering access**.

You can optionally provide a length of time, between 1 minute and 24 hours, that the product engineering access is available.

Remote Product Engineering Access (Restart required)

Disable remote product engineering access
To prevent Product Engineering remote access to the console with an exclusive user ID, select **Disable remote product engineering access**.

Note: Restart your login session for this option to take effect.

Enable remote product engineering access
To allow Product Engineering remote access to the console with an exclusive user ID, select **Enable remote product engineering access**.

Note: Restart your login session for this option to take effect.

OK
To close this window with the current selection, click **OK**.

Apply
To save the current selection without closing the window, click **Apply**.

Cancel
To close this window without saving the changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Customize Scheduled Operations

Accessing the Customize Scheduled Operations task

Use the Support Element to customize scheduled operations for automatically performing some of the following operations in the recommended process for managing internal code changes and other operations summarized in this section.

- Accept *previous* internal code changes, if any, that were retrieved, installed, and activated.
- Retrieve the new internal code changes from the support system to the Support Element.
- Install and activate concurrent internal code changes to make them operational.

You can schedule an operation to occur one time or to be repeated. You are required to specify the time and date that you want the operation to occur. If the operation is scheduled to repeat, you are asked to select:

- The day or days of the week that you want the operation to occur (optional)
- The interval or time between occurrence (required)
- The total number of repetitions (required).

Note: If you are creating a Start, Stop, or Manager Processor Sharing scheduled operation for a system on which IBM Dynamic Partition Manager (DPM) is enabled, it must be done on the Hardware Management Console. However, you can view those scheduled operations from this system.

The operations that can be scheduled on the Support Element Console are:

Activate the CPC
Makes the installed code changes operational in place of their corresponding licensed internal code. Activating the changes does not permanently modify the internal code and they may be removed until the time that they are accepted. Activating internal code changes that are not concurrent may cause the Support Element(s) to reload its licensed internal code without warning. If no licensed internal code changes are installed, the CPC will be activated with the current licensed internal code.

Note: This operation is not available when one or more managed systems have DPM enabled.

Start
Schedules an operation for starting a stopped IBM Dynamic Partition Manager (DPM) system.

Note: This operation is available only when one or more managed systems have DPM enabled.

Stop
Schedules an operation for stopping a running IBM Dynamic Partition Manager (DPM) system.

Note: This operation is available only when one or more managed systems have DPM enabled.

Deactivate (Power off) selected CPC
Stops the operating system, deallocates resources, clears associated hardware and powers off the CPC.

Note: This operation is not available when one or more managed systems have DPM enabled.

Accept internal code changes
Schedules an operation to make activated internal code changes a permanent working part of the licensed internal code of the selected CPC.

Install and activate concurrent code changes
Schedules an operation for installing and activating internal code changes retrieved for the selected CPC.

Remove and activate concurrent code changes
Schedules an operation for removing and activating internal code changed installed for the selected CPC.

Retrieve internal code changes
Schedules an operation to copy internal code changes from a remote service support system to the Support Element hard disk.

Activate or deactivate processed resources in an OOCoD record
Sends an operation to activate or deactivate a processed OOCoD record.

Note: This operation is not available when one or more managed systems have DPM enabled.

Transmit vital product data
Transmits the type of Vital Product Data (VPD) that you want transmitted to the support system.

Change LPAR Controls
Schedules an operation to change the defined capacity, WLM, absolute capping, processing weights, and initial capping value for processor types assigned to one or more active logical partitions. If a partition specified does not exist or is not active at the time the operation runs then the entire scheduled operation will not be executed (it will fail). For more detailed information, see "Change Logical Partition Controls" on page 375.

Note: This operation is not available when one or more managed systems have DPM enabled.

Change LPAR Group Controls
Schedules an operation to change a group assignment for logical partitions and to change the group capacity and absolute capping value for processor types assigned to one or more active logical partitions. For more detailed information, see "Change Logical Partition Group Controls" on page 385.

At the time this operation runs, it will fail if the following conditions are not true.

- All groups in the request must exist and contain at least one active partition.
- In order for a partition to be added to a group or removed from a group, the partition must exist and be active.

Note: This operation is not available when one or more managed systems have DPM enabled.

Audit and log management
Schedules an operation to perform an audit report on selected types of audit data. This audit data report can be viewed and offloaded to a selected media or location.

Set Power Saving
Schedules an operation to reduce the average energy consumption of a target system.

To schedule operations on the Support Element Console:

1. Open the **Customize Scheduled Operations** task.

   The Customize Scheduled Operations window displays.
2. Click **Options** from the menu bar to display the following menu options:
   - To add a scheduled operation, click **New...**.
   - To delete a scheduled operation, select the operation that you want to delete, then click **Delete**.

- To edit a scheduled operation, select the operation that you want to edit, then click **Edit**.
- To return to the Support Element console workspace, click **Exit**.

3. Click **View** from the menu bar to display the following menu options:
   - To view a scheduled operation, select the operation that you want to view, point to **View** and then click **Scheduled Details...**
   - To change the list of scheduled operations viewed within a certain time range, point to **View** and then click **New Time Range...**
4. Click **Sort** from the menu bar to sort the scheduled operations and select a sort category that you prefer.

Customize Scheduled Operations

Use this window to customize a schedule for certain operations.

Scheduled operations are helpful for situations where automatic, delayed, or repetitious processing of system operations is necessary. A scheduled operation is started at a specified time, without operator assistance to perform the operation. A schedule can be set for one operation or repeated many times.

Select a scheduled operation for an object from the list, if necessary, then select a choice from the menu bar. You can only schedule operations on Support Element objects.

Notes:

- All times displayed on the main Scheduled Operations user interface are local to the target of the operation. For example, an operation is scheduled to execute at 10:00 A.M. on a remote, managed system in a timezone that is different than where the Hardware Management Console is located. The operation will execute at 10:00 A.M. local to the remote, managed system, not at 10:00 A.M. local to the Hardware Management Console.
- If you are creating a Start, Stop, or Manage Processor Sharing scheduled operation for a system on which IBM Dynamic Partition Manager (DPM) is enabled, it must be done on the Hardware Management Console. However, you can view those scheduled operations from this system.

Click **Options** on the menu bar to select the following:

- **New...** to create a new scheduled operation
- **Delete** to remove a scheduled operation
- **Edit** to change or update the properties of a selected scheduled operation
- **Refresh** to update the current list of scheduled operations
- **Select All** to choose all scheduled operations currently displayed
- **Deselect All** to deselect all scheduled operations that were currently selected
- **Exit** to exit this task.

Click **View** on the menu bar to select the following:

- **Schedule Details...** to display schedule information for the selected scheduled operation.
- **New Time Range...** to change the list of scheduled operations viewed within a certain time range.

Click **Sort** on the menu bar to sort how you want to view the list of scheduled operations; **By Date and Time**, **By Object**, or **By Operation**.

Click **Help** to display help for the current window.

You can find more detailed help on the following elements of this window:

Options

From **Options** on the menu bar, click:

New...
To create a new scheduled operation. Adding a scheduled operation requires that you specify a type of operation, and set the schedule.

Delete
To remove the selected scheduled operations from the list. One or more scheduled operations must be selected to remove them from the list of scheduled operations, otherwise the option is unavailable. Delete a single or repeated scheduled operation when you no longer want or need the operation performed at its scheduled date and time. Deleting a repeated operation cancels all scheduled repetitions of the operation.

A confirmation window allows you to confirm or cancel your request to delete the selected operation.

Edit
To change or update the properties of a selected scheduled operation. The Edit a Scheduled Operation window is displayed. You can make any applicable updates, then click **Save** to proceed with those changes.

Note: This option is only available when you select an existing scheduled operation.

Refresh
To update the list of scheduled operations with the current schedules for the CPC. Initially, the list of scheduled operations displays the current schedules of the CPC. Afterwards, while using the task, the list is updated automatically only when you add or delete scheduled operations. But this console does not automatically update the list when the current schedule of the CPC changes. The current schedule of CPC changes when:

- A scheduled operation is performed
- Another applicable console is used to change the CPC's schedule by adding new operations or deleting operations. For example, if a Hardware Management Console is also used to monitor and operate the CPC, it can be used to change the CPC's schedule.

Refresh the list of scheduled operations, at any time, to ensure it displays the current schedule.

Select All
To select, at once, all the operations in the list.

Deselect All
To deselect, at once, all the operations in the list.

Exit
To close the window and return to the console workplace.

Sort

From **Sort** on the menu bar, click:

By Date and Time
To sort the scheduled operation list according to date in descending order with the most recent operation at the top.

By Object
To list CPCs in alphabetical order of their names, and then list each CPC's operations in alphabetical order.

Note: For consoles used to monitor and operate only one CPC, like a CPC's Support Element, selecting this choice is the same as selecting **By Operation**, which lists the operations in alphabetical order.

By Operation
To sort the scheduled operation list according to operation in alphabetical order.

Scheduled operations table

Target
Displays the name of the object the scheduled operation applies to. You can only schedule operations on Support Element objects.

Date
Identifies the day the scheduled operation will occur.

Time
Identifies the time of day the scheduled operation will occur.

Operation
Identifies the scheduled operation.

Remaining Repetitions
Identifies how many times the scheduled operation will occur.

Description
Provides a brief description of the scheduled operation.

Add a Scheduled Operation

Use this window to create a new scheduled operation for the Support Element. The list of operations available is based on the target with which the task is launched.

Select one of the objects that are listed, select an operation, then click **OK** to schedule the operation for the object.

You can schedule operations only on Support Element objects.

You can find more detailed help on the following elements of this window:

Select an Object

Select one object to assign a scheduled operation.

The first object is selected by default, but you can select any one object you want to schedule the selected operation.

Select an Operation

Accept internal code changes
Schedules an operation to make activated internal code changes a permanent working part of the licensed internal code of the Support Element and for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

Activate
Schedules an operation for activating a system.

Note: This operation is not available when one or more managed systems have DPM enabled.

Deactivate (Power off)
Schedules an operation for deactivating a system.

Note: This operation is not available when one or more managed systems have DPM enabled.

Install and activate concurrent code changes
Schedules an operation for installing and activating internal code changes retrieved for this system including a system on which IBM Dynamic Partition Manager (DPM) is enabled.

Remove and activate concurrent code changes
Schedules an operation for removing and activating internal code changes installed for this system including a system on which IBM Dynamic Partition Manager (DPM) is enabled.

Retrieve internal code changes
Schedules an operation to copy internal code changes from a remote service support system to the Support Element hard disk.

Note: This operation is available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

“Start” on page 473
Schedules an operation for starting a stopped system or partition on which IBM Dynamic Partition Manager (DPM) is enabled.

“Stop” on page 473
Schedules an operation for stopping a running system or partition on which IBM Dynamic Partition Manager (DPM) is enabled.

Single step code changes retrieve and apply
Schedules an operation to copy (retrieve) the Support Element internal code changes to the Support Element hard disk and then install (apply) the code changes.

“Transmit attestation report” on page 473
Schedules a transmittal of console firmware integrity reports to the service support system.

“Activate or deactivate processor resources in an OOCoD record” on page 473
Schedules an operation to deactivate or activate temporary processor capacity on your system. This operation is not available on a system on which IBM Dynamic Partition Manager (DPM) is enabled.

“Transmit vital product data” on page 473
Transmits the type of Vital Product Data (VPD) that you want transmitted to the support system.

“Change LPAR Controls” on page 473
Schedules an operation to change the defined capacity, WLM, absolute capping, processing weights, and initial capping value for processor types assigned to one or more active logical partitions.

Note: This operation is not available when one or more managed systems have DPM enabled.

“Change LPAR Group Controls” on page 474
Schedules an operation to change a group assignment for logical partitions and to change the group capacity and absolute capping value for processor types assigned to one or more active logical partitions.

Note: This operation is not available when one or more managed systems have DPM enabled.

Audit and Log Management
Schedules an operation to generate an audit report on selected types of audit data.

“Set Power Saving” on page 474
Schedules an operation to reduce the average energy consumption of a system component or group of components.

Note: This operation is only available when the appropriate feature is installed.

OK
To schedule the operation for the objects you have selected, click **OK**.

Cancel
To close this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Accept internal code changes

To schedule an operation to make activated internal code changes a permanent working part of the licensed internal code of the system, select **Accept internal code changes**.

Activated internal code changes are accepted only if they are more recent than internal code changes currently accepted.

Accepting internal code changes permanently modifies the licensed internal code of the system. You cannot remove accepted changes to restore the licensed internal code to a previous state.

Activate

Note: This operation is not available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

To schedule an activation of the selected object, select **Activate**.

Activating an object makes it operational.

Deactivate

Note: This operation is not available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

To schedule a deactivation of the selected object, select **Deactivate**.

Install and activate concurrent code changes

To schedule an operation for installing and activating internal code changes retrieved for this system, select **Install and activate concurrent code changes**.

Installing and activating internal code changes for the console temporarily changes the console's licensed internal code. Installing retrieved internal code changes makes them eligible for being activated. Activating installed changes makes them operational.

Note: Installing and activating the console's internal code changes requires rebooting it. Rebooting the console will temporarily prevent using it, so you should schedule this operation for a time when the console is not in use. However, if a user is logged on when this scheduled operation starts, a message will notify the user that the operation will reboot the console. The message will allow the user to choose either to continue the operation and reboot the console or to cancel the operation instead.

Remove and activate concurrent code changes

To schedule an operation for removing and activating internal code changes installed for this system, select **Remove and activate concurrent code changes**.

Removing and activating internal code changes for the console restores the licensed internal code they changed. Removing installed internal code changes restores the internal code. Then activating the restored internal code makes it operational.

Removed changes are not erased. They remain stored on the console and can be installed again at any time.

Note: Removing and activating the console's internal code changes requires rebooting it. Rebooting the console will temporarily prevent using it, so you should schedule this operation for a time when the console is not in use. However, if a user is logged on when this scheduled operation starts, a message will notify the user that the operation will reboot the console. The message will allow the user to choose either to continue the operation and reboot the console or to cancel the operation instead.

Retrieve internal code changes

To schedule an operation to copy internal code changes from a remote service support system to the Support Element hard disk, select **Retrieve internal code changes**.

Note: This operation is available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

Retrieving internal code changes makes them available for installation and activation as the working part of the licensed internal code of the system. Retrieved internal code changes do not affect the operation of the console until they are installed and activated.

To use this option, automatic dialing must be enabled for this system. Also, its remote service settings must be customized with remote service enabled and include a valid telephone number for the service support system.

Single step code changes retrieve and apply

To schedule an operation to copy (retrieve) the system internal code changes to the system hard disk and then install (apply) the code changes, select **Single step code changes retrieve and apply**.

The task:

- Verifies the system environment
- Processes a Backup Critical Data function
- Accepts all previously activated internal code changes

- Retrieves internal code changes for the support system
- Connects to the support system and downloads any internal code change **hold** status for pending internal code changes
- Installs and activates the internal code changes.

Selecting this option requires only that you set a schedule for the operation.

Start

To schedule an operation for starting a stopped system or partition on which IBM Dynamic Partition Manager (DPM) is enabled, select **Start**.

Stop

To schedule an operation for stopping a running system or partition on which IBM Dynamic Partition Manager (DPM) is enabled, select **Stop**.

Transmit attestation report

To schedule an operation for transmitting console firmware integrity reports to the support system, select **Transmit attestation report**.

The attestation report is information used by the support system to monitoring the integrity and security of protected firmware files on the Support Element.

When this operation is selected, this operation schedules transmission of an attestation report to the support system.

Activate or deactivate processor resources in an OOCoD record

Note: This operation is not available when one or more managed systems have DPM enabled.

To schedule an operation to deactivate or activate temporary processor capacity on your system, select **Activate or deactivate processor resources in an OOCoD record**.

The temporary upgrades allows you to temporarily increase, add, or replace processor capacity on your system. Retrieve, install, and activated tasks for temporary records (On/Off CoD, CBU, Planned Event, or Loaner Engine) are all separate records located on the support system or media device. Up to 4 records can be installed at any given time. You can have one On/Off CoD record installed or activated at any given time.

Transmit vital product data

To schedule an operation for transmitting vital product data from the Support Element to the support system, select **Transmit vital product data**.

When this operation is selected, this operation schedules transmission of vital product data to the support system.

Change LPAR Controls

Note: This operation is not available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

To schedule an operation to change the defined capacity, WLM, absolute capping, processing weights, and initial capping value for processor types that are assigned to one or more active logical partitions, select **Change LPAR Controls**.

Note: Depending on your user role assignment, you may only be able to view the **Change LPAR Controls** task schedule operations details.

If a specified partition does not exist or is not active at the time the operation is scheduled to run, the scheduled operation will not be executed.

You are not allowed to change the image profiles with this operation.

Note: A scheduled operation is run based on the active partitions at the time the scheduled operation is executed. It is possible to create a scheduled operation while one IOCDS is being used and to have a different IOCDS active when the scheduled operation is executed. As long as the partition names that are contained in the scheduled operation are active when the operation is scheduled to execute, it runs regardless of the IOCDS.

For more detailed information, see "Change Logical Partition Controls" on page 375.

Change LPAR Group Controls

Note: This operation is not available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

To schedule an operation to change a group assignment for logical partitions and to change the group capacity and absolute capping values for processor types that are assigned to one or more active logical partitions, select **Change LPAR Group Controls**.

Note: Depending on your user role assignment, you may only be able to view the **Change LPAR Group Controls** task schedule operations details.

At the time this operation runs, it will fail if the following conditions are not true.

- All groups in the request must exist and contain at least one active partition.
- In order for a partition to be added to a group or removed from a group, the partition must exist and be active.

It is possible to create a scheduled operation while one IOCDS is being used and to have a different IOCDS active when the scheduled operation is executed.

You are not allowed to change the image profiles with this operation.

For more detailed information, see "Change Logical Partition Group Controls" on page 385.

Audit and Log Management

To schedule an operation that generates and offloads an audit report select **Audit and Log Management**.

To generate the audit report for a scheduled operation:

- Select the report type to be generated
- Select the audit data types to be included in the report from the **Audit data types** list
- Optionally, select **Limit event based audit data to a specific number of days** and specify the number of preceding days included in the report
- Specify the FTP destination offload information for the generated audit report
- Click **Save** to include the audit data report information for the scheduled operation.

Scheduling an Audit and Log Management requires additional information on the **Options** tab in the Set up a Scheduled Operation window.

Set Power Saving

Note: This operation is only available when the appropriate feature is installed.

To schedule an operation to set power saving settings for the system, click **Set Power Saving**.

Use this operation to schedule the reduction of the average energy consumption of a system component or group of components. You can closely manage power allocations within the physical limits of your data center.

See the **Set Power Saving** task for more information.

Note: This operation fails if the configuration of the system does not match the configuration of the system when the operation was scheduled.

Details

Note: This menu choice remains unavailable until you select a scheduled operation.

Displays the schedule information for the selected operation and system.

Object
Displays the name of the object the operation is scheduled for.

Operation
Identifies the operation that is scheduled for the object.

Window begins at
Displays the date and the time of day that begins the time window in which the operation will occur.

Window length
Displays the length of the time window, in minutes, in which the operation will occur.

Remaining repetitions
Displays the remaining number of times the operation will be repeated.

Time interval between each repetition
Displays the amount of time between each repetition.

OK
To exit this window and return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

Change the Time Range

Use this window to change the subset of scheduled operations listed, to list more or fewer operations.

Initially, the list includes all scheduled operations. The time range is indefinite while all operations are listed.

To list a subset of the scheduled operations, you can specify a definite time range as a number of days, weeks, or months from the current date. Then only those operations scheduled within the time range are listed.

New Time Range
To enter a new time range, specify or click the scroll arrows to select a number (1 through 99) in the entry field, then select a unit of time for the number.

Days
To specify the time range as a number of days, select **Days**.

Weeks
To specify the time range as a number of weeks, select **Weeks**.

Months
To specify the time range as a number of months, select **Months**.

Display all scheduled operations
To list all scheduled operations, select **Display all scheduled operations**.

Note: Selecting this choice makes the **New time range** entry field unavailable.

OK
To close this window and save the changes you have made to the time range list, click **OK**.

Reset
To reset the time range list to the previously saved values, click **Reset**.

Cancel
To close this window without saving any changes and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Set up or Edit a Scheduled Operation

Use this window to set up or edit an existing scheduled operation for performing a selected operation on the selected objects.

You can only schedule operations on Support Element objects.

Click on the **Date and Time** and **Repeat** tabs to set up scheduled operations, then click **Save**. Click on the tabs to toggle between the pages. If available, click on the **Options** tab for additional parameters.

Description
Allows you to add a description of the scheduled operation in the **Description** input area. This information is displayed in the **Description** column of the "Scheduled operations table" on page 469.

"Date and Time" on page 476
Specifies the date, time, and a time window to perform a scheduled operation.

"Repeat" on page 477
Specifies the scheduled operation to be performed once or repeatedly.

"Options" on page 478
Provides additional options that you can include when scheduling certain operations.

"Single Step Settings" on page 482

Note: This tab is available when you are scheduling a **Single step code changes retrieve and apply** operation.

Allows you to choose the internal code bundle to apply.

Save
To save the settings you inputted for the set up of a scheduled operation, click **Save**.

Cancel
To discard the changes and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Date and Time

Use this page to set the date, time, and a time window to perform a scheduled operation.

Note: If you make no changes to this page, the default settings will be the current date and time, and the time window will be 10 minutes.

The time window provides a "window of opportunity" in which the scheduled operation must start. For example, if a scheduled operation requires the use of removable media, but the removable media is currently being used by another task, you can delay starting that task up to the point that it remains within the time window. If it does not start within the time window, it is marked as a failure for that iteration. If necessary, it will be scheduled for the next scheduled start, regardless of success or failure. For instance, if a Backup Critical Data operation is scheduled to start at 10:00 A.M. with a time window of 60 minutes, but the removable media is in use when the operation begins, the operation will be tried again some number of times until it begins successfully or 60 minutes elapses. If the operation does not begin successfully at 11:00 A.M., that iteration is marked as a failure. A log entry is made and the next iteration, if any, is scheduled.

Date
Set the date when you want the operation performed. Specify the month, day, and year (mm/dd/yy) or click the clock icon, using the arrows, to select the month, day, and year.

Note: When parsing dates with an abbreviated year pattern, such as "YY", the year must be interpreted relative to some century. The parsing code provided by the Java runtime does this by adjusting dates to be within 80 years before and 20 years after the current date. For example, if the current date is June 4, 2008, the string "01/11/12"would be interpreted as January 11, 2012 while the string "05/04/64" would be interpreted as May 4, 1964.

Time
Set the time when you want to begin the time window for performing the operation. Specify the hours, minutes, seconds (hh:mm:ss), and time of day (AM or PM) or click the clock icon to specify the hours, minutes, seconds, and select AM or PM.

Time Window
Select the length of time within which a scheduled operation must start. Specify how long you want to wait to try the operation again in case a scheduled operation fails; for example, if a device is not available.

Repeat

Use this page to set up a scheduled operation to be performed once or repeatedly.

Single or Repeated
Specifies whether to perform the scheduled operation once or repeatedly.

Set up a single scheduled operation
To perform the scheduled operation once, click **Set up a single scheduled operation**.

The scheduled operation is performed only once, starting at the date and time specified, and within the time window selected on the **Date and Time** page.

When this choice is selected, the other controls on this page become unavailable and cannot be used. The information is not needed for a single scheduled operation.

Set up a repeated scheduled operation
To perform the scheduled operation repeatedly, click **Set up a repeated scheduled operation**.

Select the **Days of the Week** you want to repeat the operation and specify under **Options** how often to repeat it.

A repeated scheduled operation is performed first on the selected day of the week that is on, or most closely after, the date and time specified on the **Date and Time** page. Then the operation is repeated according to the information you provide on this page.

Note: When you save these settings only one scheduled operation is created and only the next scheduled operation is displayed. You can select a scheduled operation on the main panel and select **Options** > **Edit** to see when the subsequent executions will occur or to make changes. You can also display this information by selecting **View** > **Scheduled Detatils...**.

Days of the Week
Select the day or days of the week you want to perform the scheduled operation.

Options
Specify the Interval and Repetitions and if the scheduled operation should repeat forever.

Interval
Specify or select the number of weeks to elapse before performing the scheduled operation again on each selected day.

For example, if you want the operation performed every week, on each selected day, specify 1. If you want it performed every fourth week, on each selected day, specify 4.

The interval can be from 1 to 26 weeks.

This is a required field. You must specify an interval to set up a repeated scheduled operation.

Repetitions
Specify or select the total number of times you want the scheduled operation performed.

For example, if you want the operation performed once every week for one year, select a day of the week to perform the operation, specify 1 in the **Interval** field, then specify 52 in this field for the number of repetitions.

The number of repetitions can be from 1 to 100.

This is a required field. You must specify a number of repetitions to set up a repeated scheduled operation.

Note: If **Repeat indefinitely** is selected, the **Repetitions** field is unavailable and input inhibited.

Repeat indefinitely
Select **Repeat indefinitely** if you want the scheduled operation repeated forever.

The scheduled operation is repeated at the selected interval without an end time or date.

For example, if you want the operation performed once every week forever, select a day of the week to perform the operation, specify 1 in the **Interval** field, then select **Repeat indefinitely**.

Note: If **Repeat indefinitely** is selected, the **Repetitions** field is unavailable and input inhibited.

Options

The **Options** tab is displayed for the following operations.

Activate

This page appears for the **Activate** operation.

When you want to schedule the **Activate** operation use this page to select a profile to use to perform the operation (Profile tab) and to select whether, you want an activation to start as scheduled when the system has a status of operating or exceptions (Force tab).

Note: This option is not available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

You can find more detailed help on the following elements of this window:

Profile

A profile provides additional information necessary to perform an operation. For example, scheduling an operation for activating the system requires selecting the activation profile you want used when the activation is performed.

The list displays the profiles available for the selected operation.

- **Profile** - Displays the name of the profile.
- **Description** - Displays a brief description of the profile, if available.

Force

A scheduled activation is performed unconditionally when system status is anything other than operating or exceptions. But since activation disrupts system activity, you must authorize activating a system when its status is operating or exceptions.

Select **Force a scheduled activation** to authorize activating a system even if its status is operating or exceptions.

If you do not select **Force a scheduled activation** the activation will not be started while the target has a status of operating or exceptions.

If the target status is anything other than operating or exceptions, it is activated. If the system status becomes anything other than operating or exceptions within the time window for starting the operation, it is activated.

Change LPAR Controls

This page appears for the **Change LPAR Controls** operation.

When you want to schedule the **Change LPAR Controls** operation, use this page to set scheduled defined capacity, scheduled WLM, scheduled absolute capping, weights, and initial capping value for the selected processor type (CP, ICF, IFL, zAAP, and/or zIIP). Select one or more partition names then continue to specify the wanted defined capacity, WLM, absolute capping, weight, and initial capping values in the **Defined Capacity**, **WLM**, **Scheduled Initial Weight**, **Scheduled Minimum Weight**, **Scheduled Maximum**

Weight, **Scheduled Initial Capping**, and **Absolute Capping** columns. When all the values are specified to be included in the scheduled operation, click **Save**.

Note: This option is not available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

You can find more detailed help on the following elements of this window:

Edit Absolute Capping

Use this window to specify the absolute capping of the selected logical partitions that share processors.

No change
To choose not to change the absolute capping value, select **No change**.

None
To choose not to specify absolute capping, select **None**.

Number of processors (0.01 to 255.00)
To specify the number of processors, select **Number of processors (0.01 to 255.00)** and then in the input area specify a number in the range of 0.01 to 255.00 in increments of .01.

Additional functions on this window include:

OK
To save the new values and return to the previous window, click **OK**.

Cancel
To close the window without saving the changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Change LPAR Group Controls

This page appears for the **Change LPAR Group Controls** operation.

When you want to schedule the **Change LPAR Group Controls** operation, you can use the "Capacity and Capping" on page 479 tab to verify or change the values for group capacity or absolute capping. You can also use the "Members" on page 480 tab to verify or change the group member name. When all the values are set, click **Save**.

Note: You can use the **Capacity and Capping** or **Members** tabs to update the values for capacity, capping, or group member name before this operation runs.

At the time this operation runs, it will fail if the following conditions are not true.

- All groups in the request must exist and contain at least one active partition.
- The partition must exist and be active, in order for a partition to be added to a group or removed from a group.

Note: This option is not available for a system on which IBM Dynamic Partition Manager (DPM) is enabled.

You can find more detailed help on the following elements of this window:

Capacity and Capping

The **Capacity and Capping** tab includes a table that lists the LPAR groups that might be included in this scheduled operation. Each row in the table represents a group that you might want to include for this scheduled operation. If you want to set a scheduled operation for the group capacity and absolute capping, select one or more groups. For each selection, you can "Set Group Capacity" on page 479 and "Set Group Absolute Capping" on page 480 for the processor types that are displayed in the table.

Set Group Capacity

Use this window to update the scheduled group capacity value for a selected group. The initial selection that appears in this window is the value that is displayed by the clicked hyperlink.

No change
To choose not to change the scheduled group capacity value, select **No change**.

Group capacity (0 to 2147483647)
To specify the group capacity value, select **Group capacity (0 to 2147483647)**. In the input area, specify a number in the range of 0 to 2147483647, but no more than 10 characters.

OK
To proceed with the selection and return to the previous window, click **OK**.

Cancel
To return to the previous window without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Set Group Absolute Capping

Use this window to update the group absolute capping for a selected partition. The initial selection that appears in this window is the value that is displayed by the clicked hyperlink.

No change
To keep the value of the number of processors, click **No change**.

None
To choose not to specify absolute capping, select **None**.

Number of processors (0.01 to 255.00)
To specify the number of processors, select **Number of processors (0.01 to 255.00)**. In the input area, specify a number in the range of 0.01 to 255.00 in increments of 0.01, but no more than 6 characters.

Note: This value must be a decimal number between 0.01 and 255.00 in increments of 0.01.

OK
To proceed with the selection you made and return to the previous window, click **OK**.

Cancel
To return to the previous window without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Members

The **Members** tab includes a table that lists the partition names that might be included in this scheduled operation. Each row in the table represents a partition name that you might want to include for this scheduled operation. If you want to set a scheduled operation for members, select one or more partitions. For each selection, you can set the desired group from the “Set Member Group Name” on page 480 window.

Set Member Group Name

Use this window to update the scheduled group name for a selected partition. The initial selection that appears in this window is the value that is displayed by the clicked hyperlink.

No change
To keep the value of the scheduled group name, click **No change**.

None
To choose not to specify a scheduled group name, select **None**.

Group name
To specify a scheduled group name, select **Group name**, then enter the name in the input area.

Note: The name cannot be more than 8 characters.

OK
To proceed with the selection and return to the previous window, click **OK**.

Cancel
To return to the previous window without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Audit and Log Management

This page appears for the **Audit and Log Management** operation.

When you want to set the schedule for the **Audit and Log Management** operation use this page to select the "Report type" on page 481, "Range for Event-based Audit Data Types" on page 481, "Offload information" on page 481, and "Audit Data Types" on page 481. When you set the audit and log management values, to be included in the scheduled operation, click **Save**.

You can find more detailed help on the following elements of this window:

Report type

Select the audit data type report to be generated. The supported audit data types of reports are:

HTML
HyperText Markup Language is used to generate an easily viewable report.

XML
eXtensible Markup Language is used to generate a report that is easily parsed by programs for backend processing.

Range for Event-based Audit Data Types

Use this section to limit the selected event based audit data log to a specific number of days and specifying the preceding days to be included in the audit report.

Limit event based audit data to a specific number of days
To limit the report content for the selected event based audit data types to specific number of preceding days, select **Limit event based audit data to a specific number of days**.

Number of preceding days included in report
Specify the number of preceding days used to limit the content of event based audit data types contained in the report.

Offload information

Use this section to specify the FTP destination offload information for the generated audit report.

Host or address
Specify the host name or address used for offloading the generated audit report.

User name
Specify the user name used for FTP authentication when offloading the generated audit report.

File name
Specify the file name used when the generated audit report is transferred to the specified host. The file name should include any leading directory names that may be required to correctly place the report file on the remote host. In order to be able to have periodic reports with unique names the file name can include %D, which will be replaced with the year, month, day, hour, minute, and second of when the report was generated.

Password
Specify the password used for FTP authentication when offloading the generated audit report.

Offload using secure file transfer
To enable offloading of the audit data to a secure FTP connection, select **Offload using secure file transfer**. If you are using secure FTP file transfer you must define a host key for the target system by using the **Manage SSH Keys** task.

Audit Data Types

Select the audit data types that you want included in the scheduled operations audit report from the list.

Note: The audit data types list only displays the data types that the user has authority to view. For example, the "User profiles" data type is only shown to users who are authorized to the **User Management** task.

Single Step Settings

Use this page to choose which internal code change to apply for a scheduled operation.

Apply all bundles
To choose to apply all the bundles, select **Apply all bundles**.

Apply a specific bundle
To only apply a specific bundle, select **Apply a specific bundle**.

Bundle level
Specify the bundle level in the input area.

Customize Support Element Date/Time

Accessing the Customize Support Element Date/Time task

You can use the Support Element workplace to start the task for manually setting the Support Element time-of-day (TOD) clock when the CPC does not or cannot use Server Time Protocol (STP) as a time source. The CPC is set at the next initial microcode load (IML).

To set the Support Element TOD clock:

1. Open the **Customize Support Element Date/Time** task.

   The Date and Time window displays the current date, time, and time zone offset set for the Support Element TOD clock.
2. Click **Cancel** if no corrections are necessary.
3. Enter corrections, if needed, then click **OK**.
4. Click **Refresh** to redisplay the current date, time, and time zone.
5. Click **Cancel** to close the window.

Date and Time

Use this task to configure the date, time, and time zone of the battery operated clock on the console.

Battery Operated Hardware Management Console Clock

You can change the settings under the following conditions:

- The battery is replaced in the console.
- Your system is physically moved to a different time zone.

The following fields are applicable:

Date
This field displays the current date set for the console. To change the setting, specify a new date. The default is set to the console's current date.

Set the assigned date for your system. Specify the new date using the same format as shown in the Date field. For example, `August 10, 2005`.

This information is used to establish and control operating sessions.

Time
This field displays the current time set for the console. To change the setting, specify a new time. The default is set to the console's current time.

A time is required for your local system operation.

Set the assigned time for your system. Specify the new time using the same format as shown in the Time field. For example, `8:35:00 AM`.

This information is used to establish and control operating sessions.

Time zone
To select the time zone for the console, select the down arrow on the entry field and select one. The time zone can be changed regardless of which time source you select. The default is set to the console's current time zone.

Select a city from the list that has the same time as the one you need. For example, if the console is located in Austin, Texas, select **America/Chicago** since that is the city in the list located in the same time zone as Austin.

Note: Each time zone has its own unique daylight saving time rules. Also, when you make changes to the time zone a reboot of the console is required.

Following are some examples when setting the battery operated Hardware Management Console clock.

To set the time-of day (TOD) to Local time at 8:35 am, on August 10, 2007 in Austin, the panel entries would be:

Date: `August 10, 2007`
Time: `8:35:00 AM`
Time zone: `(UTC-06:00) Central Time (US & Canada) (CST/CDT)`

To set the TOD to UTC time at 8:35 am, on August 10, 2007 in Austin, the recommended panel entries would be:

Date: `August 10, 2007`
Time: `1:35:00 PM`
Time zone: `(UTC+00:00) Greenwich Mean Time (Iceland) (UTC)`

Additional functions are available from this window:

Refresh
To redisplay the current date and time, click **Refresh**.

Cancel
To close this window and exit this task, click **Cancel**.

OK
To continue the task with the settings you have chosen, click **OK**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Customize/Delete Activation Profiles

Accessing the Customize/Delete Activation Profiles task

This task describes the **Customize/Delete Activation Profiles** task you can use to customize settings that control how the system operates. Some settings affect system operations directly, while other settings are input for other tasks you use to monitor and operator the system.

Activation profiles

Customize activation profiles to define the information that sets the operational capabilities and characteristics of the objects you want to activate. There are four types of activation profiles:

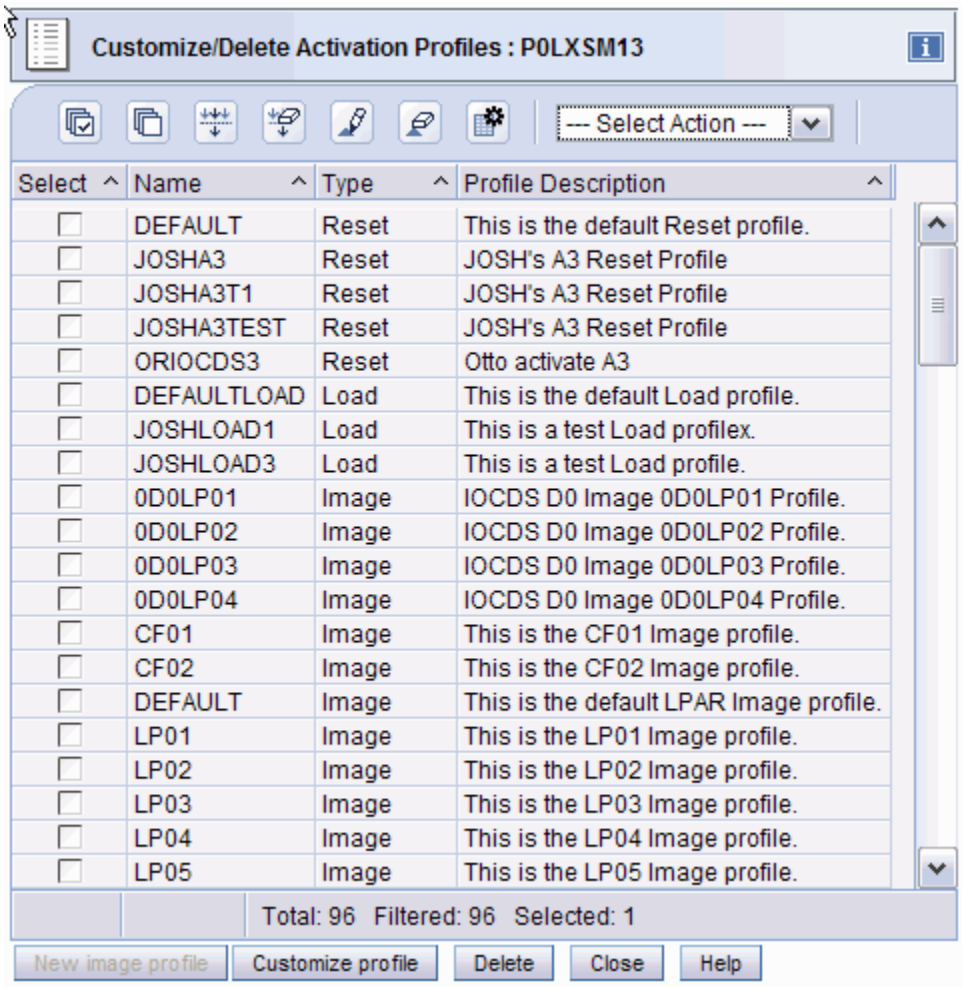


Figure 11. Activation profiles

- A *reset profile* is used to activate a central processor complex (CPC) and its images.
- An *image profile* is used to activate an image and load a control program or operating system.
- A *load profile* is used to activate an image of a CPC.
- A *group profile* is used to specify the capacity of a group of logical partitions.

A set of default activation profiles is provided with the Support Element Console Application. There is one default profile of each type:

Type	Default profile name
Reset	DEFAULT
Image	DEFAULT
Load	DEFAULTLOAD
Group	DEFAULT

The default profiles are not meant to be used to activate your central processor complex (CPC) or its images; the information in them may not be correct for your configuration or needs. Instead, customize the default profiles to meet your needs. Or customize the default profiles to meet your general needs, then use them as templates for creating new profiles that meet your specific needs.

You can perform a complete activation of a central processor complex (CPC) and its images by using a properly customized reset profile:

- When a reset profile is customized for activating the CPC, the reset profile includes the image profiles necessary to activate and load the images. That is, you can customize reset and image profiles at once for performing a complete activation of the CPC and its images:
  - Customize the reset profile for activation.
  - Customize the image profiles included in it for activating and loading one or more images during CPC activation.

You can customize load profiles and image profiles. After you use a reset profile to activate the central processor complex (CPC), you can use individual load profiles or image profiles as follows:

- You can use an image profile to activate a logical partition.

  Activating the logical partition with its image profile, rather than activating the CPC again with a reset profile, allows activating only the logical partition, while maintaining current operational capabilities and characteristics of the CPC and other logical partitions. You can activate an image this way whether you are activating it for the first time, or activating it again.
- You can use a load profile to load its image with an operating system.

  Activating the image with a load profile, rather than activating the logical partition again with an image profile, allows loading the image, while maintaining the rest of the logical partition's current operational capabilities and characteristics. You can load an image this way regardless of whether you are loading it for the first time, or loading it again but with a different operating system.

Customize unique activation profiles for each different way you want to activate the central processor complex (CPC) and its images. You can customize unique activation profiles by giving them unique names. That is, all reset profiles, load profiles, and image profiles you create must have unique names.

Recall that a reset profile includes one or more image profiles. A reset profile includes an image profile by referencing its unique profile name. While you are customizing a reset profile, you have the option of customizing the image profiles included in it. You can also customize load profiles and image profiles individually. Regardless of whether you customize them within reset profiles or individually, load profiles and image profiles remain unique.

- **Example 1:** a reset profile named LPARMODE includes image profiles named LP01 and LP02.

  While customizing the LP01 image profile individually, any changes you make also affects the LPARMODE reset profile. While customizing the LP01 image profile included in the LPARMODE reset profile, any changes you make also changes the individual LP01 image profile.

  While customizing the LP02 image profile individually any changes you make also affects the LPARMODE reset profile. While customizing the LP02 image profile included in the LPARMODE reset profile, any changes you make also changes the individual LP02 image profile.

Profiles for complete activation

A *complete activation* activates the central processor complex (CPC) and its images completely and in a single step. The result of a complete activation is an operational CPC with images loaded and running operating systems.

A properly customized reset profile includes the image profiles necessary to perform a complete activation of the CPC and its images. Using a properly customized reset profile for performing a complete activation is the recommended activation strategy for establishing the CPC's normal, day-to-day operational capabilities and characteristics.

You can perform a complete activation of a central processor complex (CPC) and its images by using a reset profile.

A complete activation means customizing a reset profile to activate the CPC, then load them with operating systems.

Staged activation

A *staged activation* activates the central processor complex (CPC) and its images in steps:

- An initial activation of the CPC and one or more images.
- And any number of subsequent, selective activations of images.

Staged activations are useful for changing the operational capabilities and characteristics of the images, but without performing a complete activation of the CPC. They allow meeting different processing needs at different times of day or on different days of the week. For example, you may want to use one logical partition as a production system during first shift, and use other logical partitions as batch and test systems on second shift.

You could perform a complete activation of the CPC each time you want to change the operational capabilities and characteristics of its images. You can get the same results by planning and performing staged activations instead. Staged activations will not require performing a complete activation of the CPC each time you want to change its operational capabilities and characteristics of its images. Instead, you can activate the CPC once, and then activate only its images when you want to change their operational capabilities and characteristics.

A reset profile is required for performing the initial activation of a staged activation. Afterwards, you can use image profiles to selectively activate logical partitions, and load profiles to selectively load images.

Information and instructions for customizing reset profiles, image profiles, and load profiles are provided in the topics that follow “Profiles for staged activations” on page 506.

Reset profiles

You can perform a complete activation of a central processor complex (CPC) and its images by using a reset profile.

A complete activation means customizing a reset profile to activate the CPC then load them with operating systems.

- See “Supporting LPAR mode operation” on page 487 , “Activating logical partitions during CPC activation” on page 492, and “Loading an operating system during activation” on page 502 along with the other topics that follow them.

Use the Support Element workplace to start the task for customizing reset profiles for a central processor complex (CPC). Starting a task is referred to also as opening a reset profile.

To open a reset profile:

1. Locate the **CPC** you want to work with.
2. Locate and open the **Customize/Delete Activation Profiles** task to start it.

   When the profile list of profiles is initially displayed, the highlighted profile is the currently assigned profile.
3. Select from the list the name of the reset profile you want to customize.
4. Click **Customize** to open the selected reset profile.

   After you start the task, use the online Help for more information about the control.

Navigating a reset profile

A reset profile includes information for activating a central processor complex (CPC) and its images.

Opening a reset profile displays its information on the windows that are organized as pages in a notebook.

The pages are identified in a profile tree view on the left side of the window with a description label. If the reset profile activates the CPC with multiple images, the profile tree view list the names of each image section with the identifying name. The information in each section is used to activate a single object either the CPC or a logical partition.

To use the profile tree view to open each page on the window:

- Click on the description label for each page within a section of the profile you want to open.
- Click on the '**+**' for each image to get a list of pages in the section of the profile.

- To save the changes made, click **Save**.
- To close the window, click **Cancel**.

Creating a new reset profile

You are responsible for creating reset profiles that meet your unique needs.

You can use the default reset profile as a template for creating new profiles. After you create a new profile, you can customize it as needed. After you create and customize your own reset profiles, you can use them as templates for creating more new profiles.

To create a new reset profile:

1. After opening and customizing a reset profile, select the General page.

   The **Profile name** field identifies the reset profile you opened. It will be used as a template for the new reset profile.
2. To use a different reset profile as a template:
3. Select the list button beside the **Profile name** field.

   This opens a list of the names of all the CPC's reset profiles. The reset profile named DEFAULT is the default reset profile provided.
4. Select from the list the name of the reset profile you want to use as a template.

   This opens the selected reset profile. Its information replaces the previous profile's information on the pages of the window.
5. Enter a unique name for the new profile in the **Profile name** field.
6. To save the profile with the new name, click **Save**.

   Note: Saving the new profile does not change the reset profile you used as a template.

Assigning a reset profile

After you open a reset profile, you can assign it to the central processor complex (CPC) as its activation profile. Whenever the CPC is activated, it is activated according to the information in its assigned activation profile.

To assign an open reset profile as a CPC's activation profile:

1. After opening and customizing a reset profile, select the General page.

   The **Profile name** field identifies the reset profile that will be assigned to the CPC.
2. To assign the reset profile as the CPC's activation profile, click **Assign profile**.

Supporting LPAR mode operation

The reset profile you use to activate a central processor complex (CPC) can establish the support required to operate the CPC. The reset profile must identify:

- An input/output configuration data set (IOCDS) that supports LPAR mode and the logical partitions you want to activate.
- LPAR mode as the operating mode you want to establish.

An IOCDS is used during a power-on reset to define your input/output (I/O) configuration to the channel subsystem of the CPC. The I/O configuration is the set of all I/O devices, control units, and channel paths available to the CPC. Performing a power-on reset also establishes the operating mode of the CPC.

To customize a reset profile to support operating the CPC:

1. Select the General page.
2. Select from the **Input/Output Configuration Data Set** list an IOCDS that defines the logical partitions you want to activate.

   Notes:

a. The **Type** column indicates the operating mode supported by each IOCDS. The column displays **Partition** to indicate an IOCDS supports LPAR mode.

b. The **Partitions** column displays the names of logical partitions supported by the IOCDS.

3. Select **Logically partitioned** from the **Mode** list as the operating mode you want to establish.

Selecting an IOCDS

The reset profile you use to activate a central processor complex (CPC) can identify the input/output configuration data set (IOCDS) you want to use. The IOCDS must be compatible with the operating mode you want to establish. That is, the IOCDS you select must support the type of operating mode you select.

An IOCDS is used during a power-on reset to define your input/output (I/O) configuration to the channel subsystem of the CPC. The I/O configuration is the set of all I/O devices, control units, and channel paths available to the CPC. Performing a power-on reset also establishes the operating mode of the CPC.

You can use the Image Profile Configuration window to:

- Set up initial parameters when you selected an IOCDS that contains two or more images that were defined in the IOCDS, but currently do not exist in the list of image profiles.
- Create one or more image using the New Image Profile Wizard when you selected an IOCDS that does not contain corresponding image profiles.

The Image Profile Configuration window allows you to automatically assign unique logical partition identifiers to each new image profile and enter a profile description to the new image profiles. You can select an existing image profile and have the existing profile's data copied to all new image profiles that are to be created.

You can customize the reset profile to use either a specific IOCDS or the active IOCDS (if you intend to use dynamic I/O configuration, for example). Follow the instructions below for using a specific IOCDS; see "Using the active IOCDS" on page 488 for more information about using the active IOCDS.

To customize a reset profile to select an IOCDS and operating mode:

1. Select the General page.
2. Select an IOCDS from the **Input/Output Configuration Data Set** list.
3. Select an operating mode from the **Mode** list that is compatible with the IOCDS you selected.

   Note the type of operating mode supported by the IOCDS you selected. The **Type** list column indicates the operating mode supported by each IOCDS:

IOCDS type	Operating mode
Partition	Logically partitioned
Currently *ID*I	The operating mode of the IOCDS is not known because the reset profile will use the active IOCDS when activation is performed; the *ID* identifies the current active IOCDS. Select an operating mode from the **Mode** list that is compatible with the IOCDS you *intend* to make active. For more information, see "Using the active IOCDS".

Using the active IOCDS

The reset profile you use to activate a central processor complex (CPC) can be customized for using the active IOCDS rather than a specific IOCDS. The *active IOCDS* is the IOCDS used for the most recent power-on reset. If you use dynamic I/O configuration, you can change the active IOCDS at any time without performing a power-on reset.

You should customize a reset profile to use the active IOCDS if you intend to use dynamic input/output (I/O) configuration. At least one of the images activated on the CPC must be loaded with an operating system that supports an application or facility for using dynamic I/O configuration. Dynamic I/O configuration is supported by:

- The Hardware Configuration Definition (HCD) application on some z/OS and OS/390 operating systems.

- The dynamic I/O configuration facility of some z/VM® and VM operating systems.

To customize an activation profile to use the active IOCDS:

1. Select the General page.
2. Select **Use active IOCDS** from the **Input/Output Configuration Data Set** list.

   When activation is performed using this reset profile:

   - The last active IOCDS is used if the CPC is not operational.
   - The active IOCDS is used if the CPC is already operational *and* if a power-on reset must be performed to make at least one other profile setting take effect. For more information, see "How using the active IOCDS affects CPC activation" on page 489.
3. Note the identifier of the IOCDS that is currently active. See **Currently ID** displayed in the **Type** list column for the **Use active IOCDS** selection. The **ID** is the IOCDS identifier.

   With dynamic I/O configuration, you can change the active IOCDS anytime prior to using this reset profile to activate the CPC.
4. Select an operating mode from the **Mode** list that is compatible with the IOCDS you've made active or *intend* to make active.

   To determine the type of operating mode supported by the IOCDS, locate it in the **Input/Output Configuration Data Set** list. The **Type** list column indicates the operating mode supported by the IOCDS.

How using the active IOCDS affects CPC activation

When a reset profile is used to activate the central processor complex (CPC), several profile settings take effect when a power-on reset is performed during activation. Such settings are referred to here as *power-on reset settings* and include, for example, the CPC's storage allocations. If the CPC is already operational and the reset profile's power-on reset settings are already in effect when activation is performed using the profile, then a power-on reset is not performed during activation. That is, a power-on reset is performed during CPC activation only if it is necessary to make one or more of the reset profile's power-on reset settings take effect.

The input/output configuration data set (IOCDS) setting is one of the reset profile's power-on reset settings, *unless* it is set to **Use active IOCDS**. Activating the CPC with a reset profile customized for using the active IOCDS affects CPC activation as follows:

- If the CPC is not operational, then a power-on reset is performed and the last active IOCDS is used.
- If the CPC is already operational, then:
  - A power-on reset is performed and the active IOCDS is used only if one or more of the reset profile's other power-on reset settings are not already in effect. For example, a power-on reset is performed if the CPC's global input/output (I/O) priority queuing flag is not the same as the global I/O priority queuing flag set in the reset profile.
  - A power-on reset is *not* performed and the active IOCDS is ignored if all of the reset profile's other power-on reset settings are already in effect.

    This may be the case when you use dynamic input/output (I/O) configuration. Using dynamic I/O to change the active IOCDS will not affect whether a power-on reset is performed during CPC activation. Only changing the reset profile's other power-on reset settings will cause a power-on reset to be performed.

Delaying the load while devices power-on

The reset profile you use to activate a central processor complex (CPC) can set a load delay for power sequencing.

Activating a CPC includes initializing its images and can include loading the images. The operating systems are loaded from devices in the input/output (I/O) configuration of the CPC.

If the devices are attached to control units that are powered-on by the CPC during activation, operating systems cannot be loaded from the devices until powering-on their control units is complete.

If you know or can estimate the amount of time it takes for control units to be powered-on, you can delay starting the load for that amount of time, up to 100 minutes. The delay may allow the powering-on to complete before the load begins.

To customize a reset profile to delay the load while control units power-on:

1. Select the General page.
2. Enter the amount of time to delay the load, from 0 to 59 seconds or 1 to 100 minutes, in the **Load delay for power sequencing** fields.

Supporting dynamic I/O configuration

The reset profile you use to activate a central processor complex (CPC) can establish the hardware support required to use dynamic input/output (I/O) configuration.

Your I/O configuration is the set of all I/O devices, control units, and channel paths you define to your hardware and software.

Performing a power-on reset establishes the *hardware I/O definition*. That is, it defines the I/O configuration to the hardware. Loading the software establishes the *software I/O definition*. That is, it defines the I/O configuration to the software.

Changing the hardware I/O definition requires performing another power-on reset, and changing the software I/O definition requires loading the software again. If the hardware and software support *dynamic I/O configuration*, you can *dynamically change* their I/O definitions. Changes made dynamically, referred to as *dynamic I/O changes*, take effect immediately. Yet they do *not* require a power-on reset or load to make them take effect.

Hardware support for dynamic I/O

Your hardware is the CPC. Dynamic I/O configuration, or simply *dynamic I/O*, is a facility of the CPC's licensed internal code. The hardware support required for using dynamic I/O can be established during power-on reset of the CPC:

- The IOCDS used during power-on reset must support dynamic I/O. The IOCDS must be either:
  - Built using the Hardware Configuration Definition (HCD) application of an z/OS and OS/390 or other operating system that supports dynamic I/O.
  - Written using the DYN option of the input/output configuration program (IOCP) utility of a z/VM and VM operating system that supports dynamic I/O.
- Dynamic I/O must be enabled for the CPC. That is, the CPC must allow dynamically changing its I/O definition.

  Note: Only a power-on reset of the CPC, performed directly or during CPC activation, can initially enable dynamic I/O. After, you can use the support element workplace at any time, if necessary, to change the dynamic I/O setting. For more information, see “Enabling or disabling dynamic I/O without performing a power-on reset” on page 491.
- Dynamic I/O must be enabled for a logical partition.

To customize a reset profile for hardware support of dynamic I/O:

1. Select the General page.
2. Select an IOCDS that supports dynamic I/O from the **Input/Output Configuration Data Set** list.

   Note: The **Allow Dynamic I/O** column displays **Yes** to indicate an IOCDS supports dynamic I/O.
3. Select the Dynamic page.
4. Mark the **Allow dynamic changes to the channel subsystem input/output (I/O) definition** check box.

The check box displays a check mark when you mark it. The check mark indicates you want to enable dynamic I/O for the CPC.

Enabling or disabling dynamic I/O without performing a power-on reset

Performing a power-on reset of the central processor complex (CPC), either directly or by activating the CPC, establishes many of its initial operational capabilities and characteristics, including whether dynamic input/output (I/O) configuration is enabled or disabled. After a power-on reset of the CPC is performed, changing its operational capabilities and characteristics requires performing another power-on reset.

If a power-on reset of the CPC initially enables dynamic I/O configuration, a task becomes available on the support element workplace for changing the CPC's dynamic I/O setting without performing another power-on reset.

To change the CPC's dynamic I/O setting without performing a power-on reset:

1. Locate the **CPC** to work with.
2. Locate and open the **Enable/Disable Dynamic Channel Subsystem** task to start it.

   The Customize Dynamic Channel Subsystem window displays.
3. Use the window's controls, as follows, to enable or disable dynamic I/O for the CPC:
   a. Review the CPC's current setting for dynamic I/O. The selected **Enabled** or **Disabled**, indicates the current setting.
   b. While dynamic I/O is enabled, select **Disabled** to change the setting to disabled.
   c. Or while dynamic I/O is disabled, select **Enabled** to change the setting to enabled.
   d. Click **OK** to save the setting and close the window.

Enabling or disabling the global input/output I/O) priority queuing

The reset profile you use to activate a CPC can enable or disable the global input/output (I/O) priority queuing.

To customize a reset profile for enabling or disabling global input/output (I/O) priority queuing:

1. Select the Options page.
2. Locate the **Enable global input/output (I/O) priority queuing** check box. Then either:
   - Mark the check box to enable global input/output priority queuing. The check box displays a check mark when you mark it.
   - Or unmark the check box to disable global input/output priority queuing. The check box becomes empty when you unmark it.

Releasing I/O reserves under error conditions

The reset profile you use to activate a central processor complex (CPC) can enable automatically resetting the input/output (I/O) interface under particular error conditions.

In a multiple CPC environment, several objects, which can be CPCs or logical partitions, may share the control units, channel paths, and I/O devices included in their I/O definitions.

The following error conditions may cause shared control units to hold reserves on their devices:

- A machine check places the CPC in a check-stopped state.
- Or the control program places an image of the CPC or a logical partition in a non-restartable wait state.

The reserves are held for the CPC or logical partition affected by the error condition. Holding reserves provides the affected object with exclusive use of devices, preventing them from being used by other objects that share the control units.

To release reserves held by shared control units assigned to an object, you must reset the I/O interface. Although resetting the I/O interface will not recover the object from its error condition, it will make the devices attached to shared control units available to other objects.

To customize a reset profile to enable automatically resetting the I/O interface:

1. Select the Options page.
2. Mark the **Automatic input/output (I/O) interface reset** check box.

   The check box displays a check mark when you mark it. The check mark indicates you want to enable resetting the I/O interface automatically.

Setting processor running time

The reset profile you use to activate a central processor complex (CPC) can set whether you or the CPC determines the processor running time.

When the CPC is activated, the logical processors of logical partitions activated without dedicated processor resources share the remaining processor resources.

Each logical processor is given the same processor running time. *Processor running time* is the amount of continuous time allowed for a logical processor to perform jobs using shared processor resources. Processor running time is referred to also as a *timeslice*.

The processor running time can be dynamically determined by the CPC. That is, the CPC can automatically recalculate the running time whenever the number of active logical processors changes.

You can set the running time to a constant amount. To get optimal use of shared processor resources, it is recommended to allow the CPC dynamically determine the running time.

To customize a reset profile to allow the CPC dynamically determine processor running time:

1. Select the Options page.
2. Locate the Processor running time group box.
3. Select **Dynamically determined by the system**.

To customize a reset profile to set a constant processor running time:

1. Select the Options page.
2. Locate the Processor running time group box.
3. Select **Determined by the user**.
4. Type the constant running time, from 1 to 100 milliseconds, in the **Running time** input field.

Note: After activating the CPC, you can use the Support Element workplace to dynamically change its settings for processor running time. See the **Change LPAR Controls** task for more information.

Setting power saving

The reset profile you use to activate a central processor complex (CPC) can set the energy management power saving option to reduce the average energy consumption of the system.

To customize a reset profile to set the power saving option:

1. Select the Options page.
2. Locate the Set Power Saving group box.
3. Select the **Custom Energy Management** radio button to use the power saving settings.
4. Select the **Emergency High Performance** radio button to override the power saving settings and use the high performance setting with no power saving.

Activating logical partitions during CPC activation

The reset profile you use to activate a central processor complex (CPC) can also activate one or more logical partitions.

To customize a reset profile to activate logical partitions during CPC activation:

1. If you have not already done so, customize the reset profile to activate the CPC. For more information, see “Supporting LPAR mode operation” on page 487.

2. Select the Partitions page.
3. Review the logical partition name in each **Partition** field.

   The fields are initialized with the names of logical partitions defined in the input/output configuration data set (IOCDS) selected on the General page of the reset profile.
4. Review the numbers in the **Order** fields beside the logical partition names.

   The fields are initialized with the default activation order of the logical partitions. The logical partition with an order of 1 will be activated first, the logical partition with an order of 2 will be activated second, and so on.
5. Optionally, enter a new order number in the **Order** field of a logical partition to change its activation order.

   Note: If you intend to operate one of the logical partitions in coupling facility mode, it should be activated first. That is, you should change the activation order of a coupling facility logical partition to 1.
6. Optionally, delete the order number of a logical partition to *not* activate it during activation of the CPC.

   Note: The names of logical partitions that are not activated will not be saved in the profile. That is, if you delete the order number of a logical partition, its name will be discarded.

The information used to activate a logical partition, though it is included in a reset profile, is actually the logical partition's image profile.

The name of an image profile is the same as the name of the logical partition it activates. So each logical partition has only one image profile.

Since each reset profile that activates a logical partition includes the logical partition's only image profile, changing the logical partition's information in any activation profile changes the same information in all the other profiles as well. That is, if you customize a reset profile for activating a logical partition, for example, changing the reset profile *also* changes the logical partition's information in its image profile *and* in every other reset profile that activates the same logical partition.

Assigning a logical partition identifier

The activation profile you use to activate a logical partition must assign it a unique logical partition identifier.

The logical partition identifier becomes part of the central processor identifier of each logical processor assigned to the logical partition. The central processor identifier is used by subsystems and control programs to distinguish between logical processors.

To customize an activation profile to assign a logical partition identifier:

1. If you opened a reset profile, select the name of the logical partition from the profile tree on the left side of the window.
2. Select the General page.
3. In the **Partition identifier** field, type the hexadecimal digit to assign as the logical partition identifier.

   Notes:

   a. The partition identifier must be unique among the identifiers of other logical partitions activated at the same time. If necessary, verify the partition identifier assigned to this image is unique by checking the **Partition identifier** fields on the General pages of the other logical partitions you intend to activate.

Selecting an operating mode

The activation profile you use to activate a logical partition must identify the operating mode you want to establish.

The operating mode describes the architecture that supports the operating system or control program you intend to load. *Coupling facility* and *Linux Only* are examples of operating modes.

To customize an activation profile to select an operating mode:

1. If you opened a reset profile, select the name of the logical partition from the profile tree from the left side of the window.
2. Select the General page.
3. Select the operating mode you want to establish from the **Mode** list.

Assigning a processor type to the logical partition

Depending on the processor installed in the CPC, you can assign a processor type to a logical partition:

- Internal Coupling Facility (ICF) processors
- Integrated Facilities for Linux (IFL) processors
- zEnterprise Application Assist Processors (zAAPs)

  Note: Available on the Hardware Management console Version 2.12.1.
- Integrated Information Processors (zIIPs)

To customize an activation profile to assign logical processors to a processor type:

1. If you opened a reset profile, select the name of the logical partition from the profile tree on the left side of the window.
2. Select the General page.
3. Select the operating mode you want to establish from the **Mode** list, select the Processor page.
4. Use the Logical Processor Assignments group box to select the type of processors you want assigned to the logical partition
5. Use the controls available to complete the logical partition assignment for the logical partition processor type.

Setting Workload Manager (WLM) controls

The activation profile you use to activate a logical partition can manage your defined capacity for a logical partition. See “Setting defined capacity” on page 500 to set defined capacity for logical partitions. Workload Manager allows you to run all of your work concurrently while allocating system resources to the most work first. Workload Manager constantly monitors your system, automatically adjusting the resource allocation as necessary.

To customize an activation profile to allow Workload Manager to manage logical partitions:

1. If you opened a reset profile, select the name of the logical partition from the profile tree on the left side of the window.
2. Select the General page.
3. Select **General**, **LINUX Only**, or **z/VM** from the **Mode** list.
4. Select the Processor page.
5. Unmark the **Initial Capping** box. If there are more than one processor types selected in the processor table, you may need to return to the Not Dedicated Processor Details for each processor type and unmark the Initial Capping box.

   Note: You cannot mark the **Initial Capping** box if the **Enable Workload Manager** is enabled. You must unmark it to allow Initial Capping to be marked.
6. Mark the **Enable Workload Manager** check box to enable Workload Manager.

   A check box displays a check mark when you mark it.
7. Enter the processing weight values for the logical partition that you want to be managed by Workload Manager.

Assigning initial logical or reserved processors

The activation profile you use to activate a logical partition can assign it initial logical or reserved processors.

An initial logical processor is the processor resource defined to operate in a logical partition as a physical central processor. Initial logical processors are the processors a control program uses to perform jobs for the logical partition.

Reserved processors can be defined at partition activation time, but not used during partition activation. The reserved processor is not available when the system is activated, but can become available during concurrent central processor (CP) upgrade.

To customize an activation profile to assign initial logical processors to a logical partition:

1. If you opened a reset profile, select the name of the logical partition from the profile tree on the left side of the window.
2. Select the Processor page.
3. Enter the number of initial logical processors to assign to the logical partition or the number of reserved processors.
4. Use the controls in the Logical processor assignment group box to allocate processor resources to logical partitions.

   Note: After activating logical partitions, you can use the Support Element workplace to dynamically change its settings for sharing processor resources. See the **Change LPAR Controls** task for more information.

Time offset

The Logical partition system time offset provides for the optional specification of a fixed time offset (specified in days, hours, and quarter hours) for each logical partition activation profile. The offset, if specified, will be applied to the time that a logical partition will receive from a Server Time Protocol (STP). This support can be used to address the following customer environment:

- Different local time zone support in multiple sysplexes using the STP Coordinated Timing Network (CTN).Many sysplexes have the requirement to run with a LOCAL=GMT setting in a sysplex (ETRMODE=YES or STPMODE=YES) where the time returned from a store clock (STCK) instruction yields local time. To fulfill this requirement, the time initialized for the STP CTN must be local time. With Logical partition time offset support, multiple sysplexes can each have their own local time reported to them from a STCK instruction if wanted. For instance, the STP CTN can be set to GMT, one set of sysplex partitions could specify a Logical partition offset minus 5 hours, and a second set of sysplex partitions could specify a Logical partition time offset of minus 6 hours.

To customize the image profile for the system time offset:

1. Open an activation profile customized for activating a CPC.
2. Select **Logical partition system time offset** in the Clock type assignment box
3. Select the Time Offset from the window tree view to set the offset and to choose how you want it applied when the logical partition's clock is set.
4. Click **Save**.
5. Activate the CPC.

Ensuring image profile data conforms to current maximum LICCC configuration

The data entered in the image profiles has to be compatible and supported by the Licensed Internal Code Configuration Control (LICCC). If image profile data changes, is imported, or the LICCC definition changes the profiles will be modified automatically to meet the new LICCC configuration. If this option is unchecked, the data entered for an image profile can be outside the valid LICCC configuration.

Note: It is recommended that image profile data conform to the current maximum LICCC configuration.

To customize the image profile to ensure the image profile data conforms to the current maximum LICCC configuration:

1. If you opened a reset profile, select the name of the logical partition from the profile tree on the left side of the window.
2. Select the General page.
3. Check **Ensure that the image profile data conforms to the current maximum LICCC configuration** to ensure that the image profile data conforms to the current maximum LICCC configuration.

Controlling access to performance data

The activation profile you use to activate a logical partition can control whether it has global access to performance data.

A logical partition has access to only its own performance data. A logical partition with global access also has access to the performance data of all other logical partitions activated on the same central processor complex (CPC). Performance data includes central processor usage and input/output processor usage by each logical partition.

To customize an activation profile to control global access to performance data:

1. If you opened a reset profile, select the page tab that displays the name of the logical partition.
2. Select the Security page.
3. Locate the **Global performance data control** check box. Then either:
   - Mark the check box to give the logical partition global access to performance data. The check box displays a check mark when you mark it.
   - Or unmark the check box to give the logical partition access to only its own performance data. The check box becomes empty when you unmark it.

Note: After activating logical partitions, you can use the Support Element workplace to dynamically change their security settings, including global performance data control. See the **Change LPAR Security** task for more information.

Controlling I/O configuration changes

The activation profile you use to activate a logical partition can control whether it can change the input/output (I/O) configuration of the central processor complex (CPC) on which it is activated.

Allowing a logical partition to change the I/O configuration enables:

- Reading and writing any input/output configuration data set (IOCDS) of the local CPC.
- Writing an IOCDS to a remote CPC.
- Using dynamic I/O configuration.
- Using the OSA Support Facility to view OSA configuration for other logical partitions.

To customize an activation profile to control changing the I/O configuration:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.
3. Locate the **Input/output (I/O) configuration control** check box. Then either:
   - Mark the check box to allow using the logical partition to change the I/O configuration. The check box displays a check mark when you mark it.
   - Or unmark the check box to prevent using the logical partition to change the I/O configuration. The check box becomes empty when you unmark it.

Note: After activating logical partitions, you can use the Support Element workplace to dynamically change their security settings, including I/O configuration control. See the **Change LPAR Security** task for more information.

Using dynamic I/O configuration

Dynamic input/output (I/O) configuration is supported by:

- The Hardware Configuration Definition (HCD) application on some z/OS and OS/390 operating systems.
- The dynamic I/O configuration facility of some z/VM and VM operating systems.

Input/output configuration control must be enabled for the logical partition that you want to use dynamic I/O configuration. That is, you must mark the **Input/output (I/O) configuration control** check box on the Security page of the activation profile used to activate the logical partition.

Authorizing control of other logical partitions

The activation profile you use to activate a logical partition can control whether it can be used to issue a subset of control program instructions to other logical partitions activated on the same central processor complex (CPC).

Allowing a logical partition to issue instructions to other logical partitions enables:

- Using it to reset or deactivate another logical partition.
- Using the automatic reconfiguration facility (ARF) to backup another logical partition.

To customize an activation profile to authorize control of other logical partitions:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.
3. Locate the **Cross partition authority** check box. Then either:
   - Mark the check box to allow using the logical partition to control other logical partitions. The check box displays a check mark when you mark it.
   - Or unmark the check box to prevent using the logical partition to control other logical partitions. The check box becomes empty when you unmark it.

Note: After activating logical partitions, you can use the Support Element workplace to dynamically change their security settings, including cross partition authority. See the **Change LPAR Security** task for more information.

Controlling use of reconfigurable channel paths

The activation profile you use to activate a logical partition can control whether it has exclusive use of its reconfigurable channel paths.

A logical partition has exclusive use of its reconfigurable channel paths only while they are configured on. If the channel paths are configured off, they can be configured on to another logical partition.

Isolating a logical partition's reconfigurable channel paths reserves them for the logical partition while they are configured off, and prevents them from being configured on to other logical partitions.

To customize an activation profile to control the use of reconfigurable channel paths:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.
3. Locate the **Logical partition isolation** check box. Then either:
   - Mark the check box to isolate the logical partition's offline reconfigurable channels paths. The check box displays a check mark when you mark it.
   - Or unmark the check box to make the logical partition's reconfigurable channels paths available to other logical partitions when the channel paths are configured off. The check box becomes empty when you unmark it.

Note: After activating logical partitions, you can use the support element workplace to dynamically change their security settings, including logical partition isolation. See the **Change LPAR Security** task for more information.

Authorizing basic counter set control

The basic counter set authorization control allows authorization to use the basic counter set in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is running.

To customize an activation profile to indicate whether authorization is allowed to use the basic counter set:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.
3. Locate the **Basic counter set authorization control** check box. Then either:
   - Mark the check box to indicate whether authorization is allowed to use the basic counter set authorization control in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is running.
   - Or unmark the check box not to allow authorization to use the basic counter set authorization control.

Authorizing problem state counter set control

The problem state counter set authorization control allows authorization to use the problem state counter set in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is in problem state.

To customize an activation profile to indicate whether authorization for problem state counter set is allowed:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.
3. Locate the **Problem state counter set authorization control** check box. Then either:
   - Mark the check box to indicate whether authorization is allowed to use the problem state counter set authorization control in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is in problem state.
   - Or unmark the check box not to allow authorization to use the problem state counter set authorization control

Authorizing crypto activity counter set control

The crypto activity counter set authorization control allows authorization to use the crypto activity counter set to identify the crypto activities contributed by the logical CPU and the blocking effects on the logical CPU.

To customize an activation profile to indicate whether authorization for crypto activity counter set authorization control:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.
3. Locate the **Crypto activity counter set authorization control** check box. Then either:
   - Mark the check box to indicate whether authorization is allowed to use the crypto activity counter set authorization control to identify the crypto activities contributed by the logical CPU and the blocking effects on the logical CPU.

- Or unmark the check box not to allow authorization to use the crypto activity counter set authorization control.

Authorizing extended counter set control

The extended counter sets authorization control allows authorization of the model-dependent extended counter set.

To customize an activation profile to indicate whether authorization for extended counter set authorization control:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.
3. Locate the **Extended counter set authorization control** check box. Then either:
   - Mark the check box to indicate whether authorization is allowed to use the extended counter set authorization control. The counters of this set are model dependent.
   - Or unmark the check box not to allow authorization to use the extended counter set authorization control.

Authorizing basic sampling control

The basic sampling authorization control allows authorization to use the basic sampling function. The sample data includes an instruction address, the primary ASN, and some state information about the CPU. This allows tooling programs to map instruction addresses into modules or tasks, and facilitates determination of hot spots.

To customize an activation profile to indicate whether authorization for basic sampling authorization control:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.
3. Locate the **Basic sampling authorization control** check box. Then either:
   - Mark the check box to indicate whether authorization is allowed to use the basic sampling authorization control function.
   - Or unmark the check box not to allow authorization to use the basic sampling authorization control.

Diagnostic sampling authorization control

The diagnostic sampling authorization control allows authorization to use the diagnostic sampling function. The sample data includes an instruction address, the primary ASN, and some state information about the CPU. This allows tooling programs to map instruction addresses into modules or tasks, and facilitates determination of hot spots.

To customize an activation profile to indicate whether authorization for diagnostic sampling authorization control:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.
3. Locate the **Diagnostic sampling authorization control** check box. Then either:
   - Select the check box to indicate whether authorization is allowed to use the diagnostic sampling authorization control function.
   - Or, unselect the check box not to allow authorization to use the diagnostic sampling authorization control.

Permit AES key import functions

The permit Advanced Encryption Standard (AES) key import functions allow you to enable the new Perform Cryptographic Key Management Operation functions of the CP Assist for Cryptographic Functions (CPACF) feature.

To customize an activation profile to permit AES key import functions:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.
3. Locate the **Permit AES key import functions** check box. Then either:
   - Mark the check box to permit AES key import functions.
   - Or unmark the check box not to permit AES key import functions.

Permit DEA key import functions

The permit Data Encryption Algorithm (DEA) key import functions allow you to enable the new Perform Cryptographic Key Management Operation functions of the CP Assist for Cryptographic Functions (CPACF) feature.

To customize an activation profile to permit DEA key import functions:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Security page.
3. Locate the **Permit DEA key import functions** check box. Then either:
   - Mark the check box to permit DEA key import functions.
   - Or unmark the check box not to permit DEA key import functions.

Allocating central storage (main storage)

The activation profile you use to activate a logical partition can allocate its storage.

The central storage allocated to a logical partition upon activation is its *initial storage*. You must allocate initial central storage to each logical partition you intend to activate.

To customize an activation profile for allocating central storage to a logical partition:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Storage page.
3. Use the Central storage group box to allocate the logical partition's central storage and to set its central storage origin.

Setting I/O priority queuing values

The activation profile you use to activate a logical partition can control the I/O priority queuing assignment of logical partitions.

To customize an activation profile for I/O priority queuing:

1. If you opened a reset profile, select the page tab that displays the name of the logical partition.
2. Select the Options page.
3. Use the controls to set minimum and maximum I/O priority queuing values.

Setting defined capacity

The activation profile you use to activate a logical partition can control the defined capacity for a logical partition. A defined capacity is the portion of your processor resources you order.

Your defined capacity can be associated with:

- A license software product. You specify a defined capacity for a product on the product certificate.
- An LPAR. You specify a defined capacity for an LPAR using the appropriate LPAR controls. A defined capacity applies to the entire LPAR, no matter how many applications it contains.

To customize an activation profile to set defined capacity:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the Options page.
3. Enter the defined capacity value for your logical partition.

Assigning Secure Service Container configuration settings

The activation profile you use to activate a logical partition can assign configuration settings of the logical partition in Secure Service Container mode. The Secure Service Container configuration settings are:

Boot selection
Before a Secure Service Container partition is restarted for the first time, all fields of activation profiles can be updated or saved.

Secure Service Container installer
This option is selected until the Secure Service Container partition is restarted and the input fields contain information that were previously defined.

Secure Service Container
This option is selected after the Secure Service Container partition is restarted. The **Reset Logon Settings** and **Reset Network Settings** can be updated after the restart.

Host name
A host name can be from one to 32 characters long. It cannot have special characters or imbedded blanks. Valid characters for a host name are numbers **0** through **9**, alphabetic, periods, colons, and minus symbols.

Master userid
Use this field to specify the master user ID for the selected firmware logical partition.

A master user ID can be from one to 32 characters long. It cannot have special characters or imbedded blanks. Valid characters for a master user ID name is numbers **0** through **9**, alphabetic, period, underscores, and minus symbol.

Master password
Use this field to specify the master password for the master user ID you specified. A master password can have a minimum of 8 characters and a maximum of 256 characters.

Confirm master password
Use this field to specify again the same master password you specified in the **Master password** field.

IPv4 gateway
Use this field to specify the default gateway IPv4 address.

IPv6 gateway
Use this field to specify the default gateway IPv6 address.

To customize an activation profile to set the Secure Service Container configurations:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. If you select SSC from the **Mode** list, select the SSC page.
3. Enter the host name, master user ID, master password, and default gateway Secure Service Container configuration settings:

Loading an operating system during activation

The activation profile you use to activate an object can also load its image with an operating system. The object is a central processor complex (CPC) activated in a logical partition.

To customize an activation profile to load an operating system during an object's activation:

1. Open an applicable activation profile:
   - If the object is a logical partition, either open a reset profile or open its image profile.

     For more information, see "Reset profiles" on page 486 or "Images profiles" on page 506.

     Note: The activation profile must *not* be customized to activate the logical partition as a coupling facility. For more information, see "Selecting an operating mode" on page 493.
2. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
3. Select the Load page.
4. Mark the **Load during activation** check box.

   The check box displays a check mark when you mark it. The check mark indicates activation will include loading the object's image with an operating system.
5. Use the other controls on the page to provide information about which operating system to load and how to load it.

Selecting a load type

The activation profile you use to load an image can set the load type to perform the load.

To customize an activation profile to set the load address and load parameter:

1. Open an activation profile:
2. If you opened a reset profile, select the name of the logical partition from the profile tree on the left side of the window.
3. Select the Load page.

   Note: If you opened a load profile, the Load page is the first and only page.
4. Locate the **Device type** controls to select the following load types:
   - Select **ECKD** device type to perform an ECKD DASD load
   - Select **SCSI** device type to perform a SCSI load (from certain types of channels)
   - Select **NVMe** device to perform a NVMe load (from certain types of adapters)
   - Select **Tape** device type to perform a Tape load.

Using dynamic I/O to set load attributes

The activation profile you use to load an image can enable using dynamic input/output (I/O) configuration, rather than the activation profile, to set the load address and load parameter used to perform the load.

The image must be activated on a CPC that supports dynamic I/O configuration. The image, or at least one of the images activated on the CPC, must be loaded with an operating system that supports an application or facility for using dynamic I/O configuration. Dynamic I/O configuration is supported by:

- The Hardware Configuration Definition (HCD) application on some z/OS and OS/390 operating systems.
- The dynamic I/O configuration facility of some z/VM and VM operating systems.

To customize an activation profile to enable using dynamic I/O to set the load address and load parameter:

1. If you opened a reset profile and the object is a logical partition, select the name of the logical partition from the profile tree on the left side of the window.
2. Select the Load page.

Note: If you opened a load profile, the Load page is the first and only page.

3. Mark the **Use dynamically changed address** check box.

   The check box displays a check mark when you mark it. The check mark indicates activation will perform each load using the load address set for the image using dynamic I/O configuration.

4. Mark the **Use dynamically changed parameter** check box.

   The check box displays a check mark when you mark it. The check mark indicates activation will perform each load using the load parameter set for the image using dynamic I/O configuration.

Setting a time limit for performing the load

The activation profile you use to load an image sets a time limit for performing the load.

A time limit, or *time-out value*, is the amount of time allowed for performing the load. The load is canceled if it cannot be completed within the time limit.

To customize an activation profile to set the time limit for performing the load:

1. Open an activation profile:
2. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
3. Select the Load page.

   Note: If you opened a load profile, the Load page is the first and only page.

4. Enter the time limit, from 60 to 600 seconds, in the **Time-out value** field.

Setting load attributes

The activation profile you use to load an image can set the load parameter attributes used to perform the load.

The *load address* is the address of the input/output (I/O) device that provides access to the operating system you want to load. The I/O device must be in the I/O configuration that is active when the load is performed. The I/O device may store the operating system or may be used to read the operating system from a storage device.

The *load parameter* is additional information operating systems support to provide you with additional control over the performance or outcome of a load. Check the configuration programming and reference documentation for the operating system to determine the load parameters that are available, and their effect on a load.

The *Time-out value* is the amount of time to allow for the completion of the load. The time-out value can be from 60 to 600 seconds. If the load operation cannot be completed within the specified time, the operation is canceled.

The *Worldwide port name* is the number identifying the Fibre Channel port of the SCSI target device. This field contains the 64-bit binary number designating the port name, represented by 16 hexadecimal digits.

The *Logical unit number* is the number of the logical unit as defined by FCP. This field contains the 64-bit binary number designating the unit number of the FCP I/O device, represented by 16 hexadecimal digits.

The *Boot record location* parameters can be specified from the volume label or be specified.

The *Boot program selector* identifies the program to load from the FCP-load device and contains a decimal value in the range from 0 to 30.

The *Boot record logical block address* is the load block address field represented by 16 hexadecimal characters, designating the logical-block address of a boot record on the FCP-load device. If no block address is specified, the logical-block address of the boot record is assumed to be zero.

The *OS specific load parameters* is a variable number of characters to be used by the program that is loaded during load. This information will be given to the IPLed operating system and will be ignored by the machine loader. The IPLed operating system has to support this.

To customize an activation profile to set the load parameters:

1. Open an activation profile:
2. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
3. Select the Load page.

   Note: If you opened a load profile, the Load page is the first and only page.
4. Enter the load parameter attributes for the selected Device type.

Using the Crypto Express feature

The activation profile you use to activate a logical partition can prepare it for running software products that utilize the Crypto Express feature. Using the feature's cryptographic facilities and functions requires customizing the logical partition's activation profile to:

- Give it access to at least one Crypto Express feature. This is accomplished by selecting from the Usage Domain Index and the Cryptographic Candidate list.
- Load it with an operating system, such as z/OS, that supports using cryptographic functions.
- Install the CP Assist for Cryptographic Facility (CPACF) DES/TDES Enablement feature if planning to use ICSF.

For more information about the cryptographic feature, see the **Cryptographic Configuration** task.

To customize an activation profile to allow a logical partition to use cryptographic facilities and functions:

1. If you opened a reset profile, select the name of the logical partition from the profile tree view on the left side of the window.
2. Select the General page.
3. Select **General**, **LINUX Only**, **z/VM**, or **SSC** from the Mode list.
4. Select **Crypto** from the profile tree view on the left side of the window. Use the controls on the Crypto page to indicate whether and how you want the logical partition to use the cryptographic functions and facilities.

   Notes:

   - If you intend to use the Integrated Cryptographic Service Facility (ICSF), see "Using the z/OS Integrated Cryptographic Service Facility (ICSF)" on page 504 for additional instructions for customizing the Crypto page.
   - If you intend to use a Trusted Key Entry (TKE) workstation to manage cryptographic keys, see "Using the Trusted Key Entry (TKE) Workstation feature" on page 505 for additional instructions for customizing the Crypto page.
   - After activating logical partitions customized to use Crypto Express feature, you can use the Support Element workplace to view the settings of the cryptographic controls set on the Crypto page of their activation profiles. See "View LPAR cryptographic controls" on page 505 for more information.
5. Customize the Load page to load an operating system that supports using cryptographic functions and facilities.

   For more information about loading an operating system, see the topics that follow "Loading an operating system during activation" on page 502.

Using the z/OS Integrated Cryptographic Service Facility (ICSF)

The z/OS Integrated Cryptographic Service Facility (ICSF) is a program product that provides secure, high-speed cryptographic services in the operating environment. You can use ICSF services for all logical partitions that are customized for using Crypto Express feature.

Note: Some functions of ICSF may fail if you do not have the CP Assist for Cryptographic Functions (CPACF) DES/TDES Enablement feature installed. See the *ICSF Application Programmer's Guide* or the *ICSF System Programmer's Guide* for complete information.

The activation profile you use to activate a logical partition can prepare it for using ICSF services. Customize the activation profiles when installing the CP Assist for Cryptographic Functions (CPACF) DES/TDES Enablement feature.

To customize an activation profile for a logical partition to use the ICSF services:

1. Customize a reset profile or image profile to configure the logical partition access to the cryptographic facilities and functions.

   For more information, see “Reset profiles” on page 486 or “Images profiles” on page 506.
2. Select the Crypto page again.
3. If you have not already set the logical partition's controls, set them now:

   a. Select a usage domain index for the logical partition to use for cryptographic functions from the **Usage domain index** list. More than one number should be selected from the **Usage domain index** when z/VM operating environment is running in the logical partition with other guests (for example, Linux) requiring access to the cryptographic hardware.

   Note: The cryptographic number, selected from the Cryptographic Candidate List, coupled with the usage domain index must be unique for each active partition.
4. Select from the Online List the number which specifies the coprocessors to be brought online at partition activation. For each number selected in the Online List, the corresponding number in the Candidate List must be selected.

Using the Trusted Key Entry (TKE) Workstation feature

A Trusted Key Entry (TKE) is a workstation application supported by ICSF to allow an alternative method of securely loading cryptographic keys (DES and PKA master keys and operational keys). A unique set of cryptographic keys is maintained for each domain index within the cryptographic facility. Only one partition can perform TKE functions at a time. The logical partition with this control is referred to as the TKE host. The other partitions that receive key updates from the TKE host are referred to as the TKE targets.

The activation profile you use to activate a logical partition can prepare it for being a TKE host or TKE target.

To customize an activation profile for a TKE host logical partition:

1. Customize a reset profile or image profile to enable the logical partition to use cryptographic facilities and functions.

   For more information, see “Reset profiles” on page 486 or “Images profiles” on page 506.
2. Select the Crypto again.
3. If you have not already set the logical partition's controls, set them now:

   a. Select a usage domain index for the logical partition to use for cryptographic functions from the **Usage domain index** list. It must be the same as the usage domain index set for the logical partition in the ICSF installation options data set.

   Note: The cryptographic number, selected from the Cryptographic Candidate List, coupled with the usage domain index must be unique for each active partition.
4. Select from the Online List the number which specifies the coprocessors to be brought online at partition activation. For each number selected in the Online List, the corresponding number in the Candidate List must be selected.
5. From the **Control domain index** list, also select each index that is the same as the usage domain index of each TKE target logical partition you want to manage through a TKE workstation connection to this TKE host logical partition.

View LPAR cryptographic controls

You can use the Support Element workplace to start the task to review information about the active logical partitions that use the Crypto Express feature assigned to them. You can review:

- A summary tab page of information on all active logical partitions.
- Individual tab pages for each logical partition's cryptographic controls.

To review the logical partition's cryptographic controls:

1. Open the **View LPAR Cryptographic Controls** task.

   The View LPAR Cryptographic Controls window displays. The window includes a summarized view tab for cryptos on all partitions and individual tabs for each logical partition's cryptographic controls.
2. Click **OK** when you have finished.

Profiles for staged activations

You can perform a staged activation of a central processor complex (CPC) and its images by using a reset profile for an initial activation of the CPC, and then using other types of profiles for selective activations of its images.

Typical staged activations include:

- Using a reset profile to initially activate the CPC and to activate and load one or more logical partitions. Then, at a later time, using load profiles to load one or more previously activated logical partitions with a different operating system, or using image profiles to activate and load one or more logical partitions not previously activated.

  This type of staged activation allows the operator to change the active logical partitions while maintaining the rest of the CPC's current operational capabilities and characteristics.

Images profiles

Customize an image profile for activating a logical partition when you want to activate only the logical partition, after the central processor complex (CPC) that supports it is initially activated.

Optionally, you can customize the image profile to also load the logical partition during activation.

Notes:

- Initially activating a CPC requires customizing and using a reset profile. For more information, see “Supporting LPAR mode operation” on page 487 and the other topics that follow.
- The name of an image profile is the same as the name of the logical partition it activates. Each logical partition has only one image profile.

  Each reset profile that activates a logical partition includes the logical partition's only image profile, so changing the logical partition's information in any activation profile changes the same information in all the other profiles as well. That is, if you customize an image profile for activating a logical partition, for example, changing the image profile *also* changes the logical partition's information in every reset profile that activates the logical partition.

The information used to activate a logical partition, though it is included in a reset profile, is actually the logical partition's image profile.

To open a logical partition's image profile:

1. Locate the **Images** you want to work with.
2. Locate the image with the same name as the logical partition.
3. Locate and open the **Customize/Delete Activation Profiles** task to start it.

   This opens the image profile and the list of load profiles you want to customize. When the list is initially displayed, the highlighted profile is the currently assigned profile for the partition.
4. Select from the list the name of the image profile you want to customize.
5. Click **Customize**.

Checking a logical partition's assigned activation profile

You can assign a logical partition either its image profile or a load profile as its activation profile. Whenever the logical partition is activated, individually rather than with the central processor complex (CPC), it is activated according to the information in its assigned activation profile.

In addition, whenever you start the task for customizing the logical partition's activation profiles, it opens the logical partition's assigned activation profile. After you start the task, you can customize its assigned activation profile. If its assigned activation profile is a load profile, you can also create new load profiles or open and customize any other existing load profiles.

For example, to customize the image profile for a logical partition, its assigned activation profile must be its image profile. You can check, and change if necessary, the logical partition's assigned activation profile before you begin customizing its profiles.

To check or change a logical partition's activation profile:

1. Locate the **Images** you want to work with.
2. Locate the image with the same name as the logical partition.
3. Click **Change options**.

   This opens the Change Object Options window.
4. Locate the **Profile name** field.

   It displays the name of the profile currently assigned as the logical partition's activation profile.
5. Locate the same name in the **Profile name** column in the list of profiles below the field. Then check the profile's type in the **Type** column.

   Note: The list includes the logical partition's image profile and all the load profiles that can be assigned to the logical partition.
6. If the assigned profile's type is **Image**, then no further action is required.

   Whenever you start the task for customizing the logical partition's activation profiles, you will be able to customize the logical partition's image profile.
7. If the assigned profile's type is **Load**, you will be able to customize only load profiles.

   To assign the logical partition its image profile instead, use the window to select and save the image profile.

Creating a new image profile

You are responsible for creating image profiles that meet your unique needs.

You can use the default image profile as a template for creating new profiles. After you create a new profile, you can customize it as needed. After you create and customize your own image profiles, you can use them as templates for creating more new profiles.

To create a new image profile:

1. Select the General page.

   The **Profile name** field identifies the image profile you opened. It will be used as a template for the new image profile.
2. To use a different image profile as a template:
3. Click the list button beside the **Profile name** field.

   This opens a list of the names of all the image profiles. The image profile named DEFAULT is the default image profile provided by IBM.
4. Select from the list the name of the image profile you want to use as a template.

   This opens the selected image profile. Its information replaces the previous profile's information on the pages of the notebook.
5. Enter a unique name for the new profile in the **Profile name** field.

6. Click **Save** to save the profile with the new name.

   Note: Saving the new profile does not change the image profile you used as a template.

Creating one or more image profiles

The New Image Profile Wizard tool can be used to configure new image profile parameters for one or more images currently selected in the IOCDS that do not have corresponding image profiles.

1. Select an image profile that is currently not created.
2. Click **New image profile**.
3. Use the New Image Profiles Wizard to create data for the image profile that you selected.
4. Complete the requested information for the image profile you are creating.
5. Click **Finish** to confirm your changes.

Customize multiple image profiles

The Customize Image Profile Wizard tool can be used to modify parameters for two or more of the image profiles that you select on the customize/delete activation profiles list.

1. Select two or more image profiles that you want to change parameters.
2. Click **Customize profile**.
3. Select the profiles you want to customize from the menu list. Then click **OK**.
4. Use the Customize Multiple Image Profile Wizard to modify data for two or more of the image profiles that you selected.
5. Click **Next** to start.
6. Check the appropriate check box that you want to make changes.
7. Click **Finish** to confirm your changes.

Saving an image profile

You must save an image profile to save the information you customized on its pages.

To save an open image profile:

1. After opening and customizing an image profile, select the General page.

   The **Profile name** field identifies the image profile that will be saved.
2. Click **Save** to save the image profile and close it.

Load profiles

Customize a load profile for loading an object when you want to only load the object after it is initially activated.

Customize a load profile for loading a logical partition when you want to only load the logical partition again, after it is initially activated on a CPC activated.

Note: Initially activating a logical partition requires customizing the reset profile that activates the CPC. For more information, see “Supporting LPAR mode operation” on page 487, and “Activating logical partitions during CPC activation” on page 492 along with the topics that follow.

To open a load profile:

1. Locate the **CPC** to work with.
2. Locate and open the **Customize/Delete Activation Profiles** task to start it.

   This opens the profile list that you want to customize. When the list of profiles is initially displayed, the highlighted profile is the currently assigned profile for the object.
3. Select from the list the name of the load profile you want to customize.
4. Click **Customize**.

This opens the selected load profile.

Choosing a load type: ECKD, SCSI, NVMe, or Tape

The activation profile you use to load a central processor complex (CPC) can perform a **ECKD**, **SCSI**, **NVMe** or **Tape** load.

1. Locate the **Device type** controls to select the following load types:
   - Select the type of device to perform a load for the logical partition:

     ECKD
     To perform an IPL on the logical partition from ECKD DASD device type, click **ECKD**.
   - **SCSI**
     To perform an IPL on the logical partition from SCSI device type, click **SCSI**.

     NVMe
     To perform an IPL on the logical partition from NVMe device type, click **NVMe**.

     Tape
     To perform an IPL on the logical partition from Tape device type, click **Tape**.
   - Select **SCSI** or **NVMe** to perform a SCSI (from certain types of channels) or NVMe (from certain types of adapters).

     Note: If you intend to clear main memory before loading, select **Clear the main memory on this partition before loading it**.

Performing store status before a ECKD or Tape load

The activation profile you use to load a central processor complex (CPC) can perform the store status function before performing a standard load.

The store status function stores the current values of the processing unit timer, the clock comparator, the program status word, and the contents of the processor registers in their assigned absolute storage locations.

Note: For this reason, store status can be performed only before a **ECKD** and IPL type **CCW** or **Tape** load.

Attention: Do *not* customize an activation profile to perform store status if the profile is customized to load an operating system that already automatically performs store status upon being loaded.

To customize an activation profile to perform store status before a **ECKD** and IPL type **CCW** or **Tape** load:

1. Select the Load page.

   Note: If you opened a load profile, the Load page is the first and only page.
2. Locate the **Device type** controls. Select **ECKD** and IPL type **CCW** or **Tape** to perform a load from a device.
3. Ensure the Load type is set to **Load a dump program** to clear main storage on the logical partition before loading..
4. Mark the **Store status** check box.

   The check box displays a check mark when you mark it. The check mark indicates activation will perform the store status function before performing the load.

Creating a new load profile

You are responsible for creating load profiles that meet your unique needs.

You can use the default load profile as a template for creating new profiles. After you create a new profile, you can customize it as needed. After you create and customize your own load profiles, you can use them as templates for creating more new profiles.

To create a new load profile:

1. Locate the **Profile name** field.

The field identifies the load profile you opened. It will be used as a template for the new load profile.

2. To use a different load profile as a template:
   a. Select the list button beside the **Profile name** field.

      This opens a list of the names of all the load profiles. The load profile named DEFAULTLOAD is the default load profile provided.

   b. Select from the list the name of the load profile you want to use as a template.

      This opens the selected load profile. Its information replaces the previous profile's information on the notebook page.
3. Enter a unique name for the new profile in the **Profile name** field.
4. Click **Save** to save the profile with the new name.

   Note: Saving the new profile does not change the load profile you used as a template.

Assigning a load profile

After you open a load profile for an object, either a central processor complex (CPC) or logical partition, you can assign it to the object as its activation profile. Whenever the object is activated, it is activated according to the information in its assigned activation profile.

To assign an open load profile as an object's activation profile:

1. After opening and customizing a load profile, the **Profile name** field identifies the load profile that will be assigned to the object.
2. Select the **Assign profile** push button to assign the load profile as the object's activation profile.

Saving a load profile

You must save a load profile to save the information you customized on its page.

To save an open load profile:

1. After opening and customizing a load profile, the **Profile name** field identifies the load profile that will be saved.
2. Click **Save** to save the load profile and close it.

Group profile

Customize a group profile for activating a logical partition group after the central processor (CPC) that supports it is initially activated.

To open a group profile:

1. Locate the **CPC** to work with.
2. Locate and open the **Customize/Delete Activation Profiles** task to start it.

   This opens the profile list that you want to customize. When the list of profiles is initially displayed, the highlighted profile is the currently assigned profile for the object.
3. Select from the list the group profile to customize.
4. Click **Customize**.

   This opens the selected group profile.

Creating a new group profile

To customize a logical partition group name, enter a new name in the field. To view or customize an exiting logical partition group name, select the arrow beside the field to list the names of existing group names.

You can use the default group name as a template for creating a new group name.

To create a new group name:

1. The **Group name** field identifies the group profile name. It can be used as a template for the new group name.
2. Click the list button beside the **Group name** field to use a different group name as a template.

   This opens a list of the names of all the group names. The group named DEFAULT is the default group name provided.
3. Select from the list the name of the group you want to use as a template.
4. To create a new group name, enter a unique name for the new logical partition in the **Group name** field.
5. Enter a description of the new group name in the **Group description** field.
6. Click **Save** to save the group profile with the new.

Setting a group capacity value

The group capacity value can be specified in determining allocation and management of processor resources assigned for a logical partition group. The activation profile you use to activate a logical partition group can control the defined capacity for the logical partition group.

To customize an activation profile to set group capacity:

1. Enter the group capacity value for your logical partition group.
2. Click **Save** to store the values.

Setting an absolute capping value

The absolute capping value can be specified in determining allocation and management of processor resources assigned for a logical partition group. The activation profile you use to activate a logical partition group can control the defined absolute capping value for the logical partition group. The absolute capping can be None or a number of processors value from 0.01 to 255.0.

To customize an activation profile to set absolute capping:

1. In the processor type table, select the current absolute capping setting in its field.
2. Use the Customize Group Profiles window to specify the absolute capping for the selected processor type.
3. Click **Save** to store the values.

Grouping the CPC for complete activation

You can customize more than one reset profile for performing complete activations of the CPC and its images. You can customize a reset profile for a complete activation of the CPC.

To use a reset profile for activating the CPC, you must assign it to the CPC before performing the activation. Afterwards, to use a different reset profile for activating the CPC, you could assign it to the CPC, replacing the previously assigned profile.

Rather than changing the reset profile assigned to a CPC each time you want to use a different one, you can instead create a unique group with the CPC for each reset profile you want to assign to it.

To assign the CPC a reset profile for activating it:

1. Create a group with the CPC for activating it:
   a. Give the group a meaningful name, like LPARMODE.
   b. Assign the group's CPC the reset profile for activating it in LPAR mode.

Then to activate the CPC with either profile, simply activate the appropriate group.

Grouping the CPC for staged activations

You can customize a reset profile for performing an initial activation of the CPC and customize a load profile for performing a subsequent activation that only loads it. For example, you may:

- Customize the reset profile to activate the CPC and load the operating system used for production.
- And customize the load profile to only load the CPC with the operating system used for performing dumps.

To use the reset profile for activating the CPC, you must assign it to the CPC before performing the activation. Afterwards, to use the load profile for activating the CPC, you could assign it to the CPC, replacing the previously assigned profile.

Rather than changing the activation profile assigned to a CPC each time you want to use a different one, you can instead create a unique group with the CPC for each activation profile you want to assign to it.

For example, to assign the CPC both a reset profile for activating it initially, and a load profile for only loading it:

1. Create a group with the CPC for activating it initially:
   a. Give the group a meaningful name, like PRODUCTION.
   b. Assign the group's CPC the reset profile.
2. Create another group with the CPC for only loading it:
   a. Give the group a meaningful name, like LOADFORDUMP.
   b. Assign the group's CPC the load profile.

Then to activate the CPC with either profile, simply activate the appropriate group.

Grouping images for staged activations

You can customize more than one activation profile for performing staged activations of the CPC and its images. For example, you may:

- Customize a reset profile for an initial activation of the CPC, with support for activating three logical partitions, but initially activating only of one of the logical partitions to support your production environment.
- And customize image profiles for activating the other two logical partitions to support batch processing and testing environments.

Using the reset profile for activating the CPC and one logical partition still automatically assigns *each* logical partition an image profile of the same name as its activation profile. Afterwards, you may want to deactivate the first logical partition, and then activate the other two logical partitions.

To help distinguish between the different purposes of the logical partitions, you can create a unique group with the logical partitions that support each purpose.

So, for example, to use one logical partition for production, and the other two logical partitions for batch processing and testing:

1. Create a group with the logical partition used for production.

   Give the group a meaningful name, like PRODUCTION.
2. Create another group with the logical partitions used for batch processing and testing.

   Give the group a meaningful name, like BATCHANDTEST.

Then to establish either environment, simply activate the appropriate group after deactivating the other group.

Note: The logical partitions in either group will be activated according to the information in the image profiles automatically assigned to them by the initial activation of the CPC.

Customize/Delete Activation Profiles

Use this task to view, change, create, or delete activation profiles for the central processor complex (CPC) and their images.

There are four types of activation profiles:

- Reset profile used to activate a CPC and its images
- Load profile used to activate image and load a control program or operating system.
- Image profile used to activate an image of a CPC
- Group profile used to specify the capacity of a group of logical partitions.

Save
To save the current information and settings as an activation profile for the CPC, click **Save**.

Copy Profile
To put the current profile information and settings in a temporary storage area to make it available to other profiles and objects on the console, click **Copy Profile**.

Paste Profile
To retrieve the information and settings currently in the temporary storage area for the current profile type, click **Paste Profile**.

Assign Profile
To assign the current profile to the object, to use it to activate the object whenever activation is started from the console, click **Assign Profile**.

Cancel
To close the profile without making changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following:

Profile Tree

This lists all pages for the current profile and a list of referenced profiles and their pages.

Reset pages

This type of activation profile, referred to also as a reset profile, includes all the information necessary to activate a CPC and each image supported by the CPC.

Make a selection from the Profile Tree to view the CPC pages:

General
To describe the selected reset profile and its purpose, and to identify the Input/Output (I/O) configuration and operating mode to establish for the CPC activated by the profile, select **General**.

Storage
To customize the storage configuration to establish for the CPC activated by the profile, select **Storage**.

Dynamic
To customize information that controls whether the Input/Output (I/O) configuration established for the CPC activated by the profile can be dynamically changed, select **Dynamic**.

Options
To enable or disable global input/output (I/O) priority queuing and customize options for error handling and recovery for the CPC activate by the profile, select **Options**.

Fenced
To display the number of available processors when a book is fenced and to determine the processor assignment, select **Fenced**.

Partitions
To customize a list of logical partitions to activate, and the order in which they are activated, on the CPC activated by the profile, select **Partitions**.

Note: The CPC pages include this additional page if the operating mode selected on the **General** CPC page is logically partitioned (LPAR) mode.

The window includes a section of image pages for each logical partition listed on the **Partitions** page. The information in each section is used to activate the multiple images supported by the CPC.

General

Use this window to describe the selected profile and its purpose and to identify the Input/Output (I/O) configuration and operating mode to establish for the Central Processor Complex (CPC) activated by the profile.

Note: An activation profile used to activate a CPC is also referred to as a reset profile.

Profile name

Specify or select the name of the profile you want to work with:

- To customize a new profile, you can immediately edit the value that currently appears in the input field or you can select an item that appears in the drop-down list.
- To view or customize an existing profile, select the arrow beside the field to list the names of existing profiles. Then select a profile name from the list to display its information.

A profile name is required to save the information.

A profile name can be from 1 to 16 characters long. It cannot have special characters or imbedded blanks. Valid characters for a profile name are:

Characters 0 through 9
Decimal digits

Characters A through Z
Letters of the English alphabet

Note: Profile names are not case-sensitive. All alphabetic characters are saved in uppercase.

Description
Include a brief note, up to 50 characters long, that describes the contents or purpose of the profile.

Note: A description is recommended, but optional.

IOCDS table

Select an Input/Output Configuration Data Set (IOCDS) to use during activation to define the Input/Output (I/O) configuration for the Central Processor Complex (CPC).

The I/O configuration is the set of all I/O devices and channel paths available to the CPC.

Input/Output Configuration Data Set
Displays the data set identifier and name of the IOCDS.

Type
Identifies the operating mode supported by the IOCDS. This must match the operating mode selected in **Mode**.

Note: Activation will fail if a mismatch exists between an IOCDS and mode.

Allow Dynamic I/O
Indicates whether the IOCDS defines an I/O configuration that supports dynamic changes.

Partitions
This column displays the names of logical partitions supported by the IOCDS.

Mode

Select the operating mode to establish during activation to support the number and type of control programs that can operate on the Central Processor Complex (CPC).

The mode determines some of the other types of information included in the reset profile. Different profile information is associated with each different mode. Only profile information associated with the selected mode will be saved.

Note: Activation will fail if a mismatch exists between an IOCDS and mode.

Load Delay for Power Sequencing

Specify the amount of time to delay between completing power-on reset and performing a load.

The delay can be specified at a maximum of 100 minutes, 0 seconds.

This delay allows Input/Output (I/O) devices to power-on before the load starts.

You can find more detailed help on the following elements of this window:

Image Profile Configuration

Use this window to set up initial parameters when you select an IOCDS that contains two or more images that were defined in the IOCDS, but currently do not exist in the list of image profiles. The default image profile can be used as a template for creating the set of new image profiles.

You can select one of the following options to:

- Automatically creating all new images using the choices specified on this panel, or
- Create each individual image profile using the *New Image Profile Wizard*.

You can select one or more of the following options to apply to all new image profiles:

- Automatically assign unique logical partition identifiers to each new image profile which saves you the need to determine which logical partition identifiers are available for this IOCDS.
- Allows you to assign a profile description to each of the new image profiles. You can insert the logical partition name into the description by using the %NAME parameter. If you want to specify the %, you must type %%.
- Allows you to select an existing image profile and have the existing profile's data be copied to all new image profiles that are to be created.

OK
To apply the selected changes, click **OK**.

Cancel
To close the window without making a selection, click **Cancel**.

Help
To display help for the current window, click **Help**.

Storage

This window displays the storage available for allocating to the CPC's logical partitions. The **Mode** list in **General** of this reset profile identifies the operating mode you selected for activating the CPC.

Installed storage details

Displays the CPC's total amount of storage available for allocating to the CPC's logical partitions.

Customer storage
Displays the storage amount available for allocating to the Central Processor Complex's (CPC) logical partitions.

To customize each logical partition's storage configuration, select its image profile, then select **Storage**.

Dynamic

Use this window to customize information that controls whether the Input/Output (I/O) configuration established for the Central Processor Complex (CPC) activated by the profile can be dynamically changed.

Dynamic I/O

This window allows you to customize the Input/Output (I/O) configuration established for the Central Processor Complex (CPC) activated by the profile.

To set whether the I/O definition established for the CPC activated by the profile can be dynamically changed, select **Allow dynamic changes to the channel subsystem input/output (I/O) definition**.

If this is selected it indicates activating this profile establishes an I/O definition that can be dynamically changed. That is, dynamic I/O will be enabled. Otherwise, this indicates the I/O definition cannot be changed dynamically. That is, dynamic I/O will not be enabled.

The input/output (I/O) definition is the set of all I/O devices and channel paths available to a central processor complex (CPC). An input/output configuration data set (IOCDS) is used during power-on reset as the source of the I/O definition.

Ordinarily, changing the I/O definition requires performing a power-on reset with a modified or different IOCDS. Dynamically changing the I/O definition does not require a power-on reset.

Dynamically changing the I/O definition requires support from the selected IOCDS and from the Hardware Configuration Definition (HCD) feature of a Multiple Virtual Storage (MVS™) operating system.

Then the I/O definition can be changed dynamically by using the HCD feature of MVS.

Note: The active IOCDS must also support dynamically changing the channel subsystem I/O definition.

Options

Use this window to enable or disable the global input/output (I/O) priority queuing, customize options for error handling and recovery, and set power saving for the Central Processor Complex (CPC) activated by the profile.

Enable global input/output I/O priority queuing

To enable or disable global I/O priority queuing dynamically after initial microcode load (IML), select **Enable global input/output I/O priority queuing**.

Global I/O priority queuing allows the operating system to specify a priority to be associated with an I/O request at Start Subchannel time. These values are passed to the I/O subsystem for use when making queuing decisions with multiple requests.

Automatic input/output (I/O) interface reset

To indicate whether the I/O interface is reset automatically when any condition occurs that causes shared control units to hold reserves on their devices, select **Automatic input/output (I/O) interface reset**.

- A machine check places the Central Processor Complex (CPC) in a check stopped state.
- A control program places a logical partition in a non-restartable wait state.

If selected, the I/O interface is reset automatically if any of the listed conditions occurs. Otherwise, this indicates the I/O interface is not reset automatically.

In a multiple CPC environment, several objects, which can be CPCs or logical partition, may share the control units, channel paths, and I/O devices included in their I/O interfaces.

Each condition listed above causes shared control units to hold reserves on their devices for the object affected by the condition, Holding reserves provides the affected object with exclusive use of devices, preventing them from being used by other objects that share the control units.

Resetting the I/O interface releases reserves held by shared control units assigned to an object. Their devices become available to other objects.

Note: Automatically resetting the I/O interface will not recover the object from any of the conditions.

Processor running time

If the profile activates the Central Processor Complex (CPC), use this section to indicate how processor running time is determined.

Processor running time is the amount of continuous time allowed for logical processors to perform jobs on shared processors. The amount of continuous time is also referred to as a timeslice.

Dynamically determined by the system

To have the CPC calculate the running time whenever the number of active logical processors changes, select **Dynamically determined by the system**.

Note: When processor running time is dynamically determined, it reduces the possibilities for suboptimal use of processor resources.

Determined by the user
To have this profile set a constant running time, select **Determined by the user**. Then specify the time in the **Running time** field.

Running time

When the processor running time is determined by the user through this profile, type the constant amount of running time set for logical processors to perform jobs on shared processors in the **Running time** field.

The running time can be from 1 to 100 milliseconds.

The running time specified is assigned to all logical processors shared by logical partitions activated without dedicated processing resources. Each logical partition has control of shared processor resources for the specified running time. Control passes to the next logical partition when the running time interval expires.

Note: This field is applicable only when **Determined by the user** is selected. Otherwise, this field is unavailable.

System Recovery Time

Use this section to indicate whether there is a limit on the amount of time the Central Processor Complex (CPC) is allowed to spend on error handling and recovery.

Limit system recovery time

If recovery time is limited, specify the amount of time the Central Processor Complex (CPC) is allowed to spend on error handling and recovery before it is put into a checkstop state.

The time limit can be from 1 to 999 seconds.

The amount of time determines the type of recovery that is attempted. If recovery time is not limited, then all types of recovery are attempted.

Note: This field is applicable only **Limit system recovery time** is selected. Otherwise, this field is unavailable.

Time limit

If recovery time is limited, specify the amount of time the Central Processor Complex (CPC) is allowed to spend on error handling and recovery before it is put into a checkstop state.

The time limit can be from 1 to 999 seconds.

The amount of time determines the type of recovery that is attempted. If recovery time is not limited, then all types of recovery are attempted.

Note: This field is applicable only **Limit system recovery time** is selected. Otherwise, this field is unavailable.

Set Power Saving

Use this window to select the energy management power saving option for the CPC upon performing the power-on reset. Power saving is used to reduce the average energy consumption of the system.

Custom energy management

Emergency high performance
To use the high performance setting with no power saving, select **Emergency high performance**.

Display fenced book page
Check this option to display the Fenced window.

Fenced CPC drawer

This window allows you to determine how the available system processors would be assigned when a hardware problem occurs with one of the CPC drawers that causes the system to be fenced or become unavailable for use.

- **Number of available processors for Licensed Internal Code** indicates the number of processors that are available in your system.
- **Number of available processors when a CPC drawer is fenced** indicates the number of processors that your system can use when one system drawer is fenced from use.
- **Number of available processors when a XX processors drawer is fenced** where XX indicates the number of processors that your system can use when the specified processors drawer is fenced from use.

Processors assignment controls

Select a processor assignment option.

Determined by the system
Select this option if you want the system to determine how to assign all available processors when a drawer is fenced from use in your system.

Determined by the user
Select this option if you want to manually assign the processors to your system when a drawer is fenced from use.

Processor assignments

Display processor assignment when a XX processors drawer is fenced
Where XX indicates the number of processors fenced from use. Select this option to display the processor assignments

Processor type
Displays the physical processor assigned to the logical partitions logical processors

LICCC Definition
Displays the amount of licensed internal code installed in your system

Value used when CPC drawer is Fenced
Indicates how many processors have been assigned to the specified processor types.

Partitions

Use this window to customize a list of logical partitions to be activated and the order in which they are activated on the Central Processor Complex (CPC) activated by the profile.

To activate a logical partition, you must provide its name **and** activation order. Logical partitions with blank activation orders will not be activated and their names on this page will not be saved in the profile.

Partition
Specify the names of the logical partitions to activate.

Order
Specify the numeric positions of the logical partitions in the activation order.

Important: Logical partitions activated in coupling facility mode, if any, should be activated first.

For each logical partition to be activated, customize the information for activating it in its corresponding set of image pages. To display the image pages for a logical partition, select its pages from the profile tree view on the left side of the window.

Load

Use this window to customize information that controls loading a control program for the logical partition activated by the profile.

Use this window to customize information that controls loading a control program for the logical partition activated by the profile.

Note: The images pages do not include this additional page if the operating mode selected on the **General** image page is Coupling facility or SSC mode.

Profile name

Specify or select the name of the profile you want to work with:

- To customize a new profile, specify a new name in the field.
- To view or customize an existing profile, select the list button beside the field to list the names of existing profiles. Then select a profile name from the list to display its information on the window.

A profile name is required to save the information on the window.

A profile name can be from 1 to 16 characters long. It cannot have special characters or imbedded blanks. Valid characters for a profile name are:

Characters 0 through 9
Decimal digits

Characters A through Z
Letters of the English alphabet

Note: Profile names are not case-sensitive. All alphabetic characters are saved in uppercase.

Description
Enter a brief note, up to 50 characters long, that describes the contents or the purpose of the profile. A description is recommended, but optional.

Device type
Select the type of device to perform a load for the logical partition. You would use the SCSI or NVMe option to do a standalone dump to a SCSI device or NVMe adapter.

ECKD
To perform an IPL on the logical partition from ECKD DASD device type, click **ECKD**. Optionally, select **Load a dump program** load type to the clear main storage on the logical partition before loading.

SCSI
To perform an IPL on the logical partition from SCSI device type, click **SCSI**.

NVMe
To perform an IPL on the logical partition from NVMe device type, click **NVMe**.

Tape
To perform an IPL on the logical partition from Tape device type, click **Tape**. Optionally, select **Load a dump program** load type to the clear main storage on the logical partition before loading.

IPL type:
Select the type of IPL for the selected **ECKD** device type to perform for the logical partition.

Channel Command Word (CCW)
To perform the load on CCW IPL, click **Channel Command Word (CCW)**.

List-directed
To perform the load on a list-directed IPL, click **List-directed**.

If the selected device type is **SCSI**, **NVMe**, or **Tape** this field is unavailable.

Load type:
Select the type of load to perform for the logical partition. Optionally, for **ECKD** or **Tape** select clear main the memory before loading. You would use the **ECKD** or **Tape** option to do a standalone dump and select the **Load a dump program** option.

Load an OS
To perform an operating system load type on the logical partition, click **Load an OS**.

Load a dump program
To perform a dump program load type on the logical partition, click **Load a dump program**.

Validation:

Enable Secure Boot
To verify the signature of the load program and distributor's signature match, select **Enable Secure Boot**.

Certificates
The Certificates table displays all the certificates assigned to the partitions.

If the selected device type is **Tape** or **ECKD** and IPL type **CCW** is selected this field is unavailable.

Options:

Store status
The store status function stores the current values of the processing unit timer, the clock comparator, the program status word, and the contents of the processor registers in their assigned absolute storage locations.

If the **Load a dump program** type is selected, click the check box to change the setting.

- A check mark indicates performing the store status function before the load.
- An empty check box indicates not performing the store status function before the load.

Clear the main memory before loading
Select this to clear main memory storage on the logical partition before a load. Clearing partitions with larger amount of main memory storage may take longer.

If the selected device type is **SCSI** or **NVMe** this field is unavailable.

Load address:

Enter the address of the input/output (I/O) device that provides access to the control program to load. For a SCSI load or NVMe load, this field has the device number of the device (for example, fibre channel adapter) that is used to perform the SCSI or NVMe load. This should contain four hexadecimal digits for NVMe load or five hexadecimal digits for SCSI load.

A load address is required.

The source of the control program must be an I/O device in the I/O configuration that is active when this profile is activated. The I/O device can store the control program or can be used to read the control program from a data storage medium.

Note: This field is applicable only when **Use dynamically changed address** check box is empty. Otherwise, if the check box displays a check mark, this field is unavailable.

Use dynamically changed address

To indicate whether the load address is dynamically determined by changes to the channel subsystem Input/Output definition (I/O), select **Use dynamically changed address**.

If this is selected, the load address is dynamically determined. Otherwise, this profile sets the load address. See the **Load address** field for the address set by this profile.

Specify the address in the **Load address** field.

Load parameter:

Specify the optional information, if any, to use to further control how the control program is loaded during activation. Valid characters for a load parameter are:

- At (@)
- Pound (#)
- Dollar ($)

- Blank character
- Period (.)
- Decimal digits 0 through 9
- Capital letters A through Z .

Some control programs support the use of a load parameter to provide additional control over the performance or outcome of a load. Check the configuration programming and reference documentation for the control program to determine the load parameters that are available and their effects on a load.

Note: This field is applicable only when **Use dynamically changed parameter** is **not** selected. Otherwise, this field is unavailable.

Use dynamically changed parameter

To indicate whether the load parameter is dynamically determined by changes to the channel subsystem Input/Output (I/O) definition, select **Use dynamically changed parameter**

If this is selected, the load parameter is dynamically determined. Otherwise, this profile sets the load parameter. Enter the parameter for this profile in the **Load parameter** field.

Time-out value:

Specify the amount of time to allow for the completion of the load.

The time-out value can be from 60 to 600 seconds. If the load operation cannot be completed within the specified time, the operation is canceled.

If the selected device type is **SCSI**, **NVMe**, or **ECKD** and IPL type **List-directed** is selected, this field is unavailable.

Boot record location:

The boot record location (C,H,R format) parameters can be specified from the volume label or be specified.

- Select **use volume label** to specify the boot record label from the volume label
- Select to specify the C,H,R format. The Cylinder number is a 4-byte value ranging from '0x00000000' to '0x0FFFFFFF'. The Head number is a 1-byte value ranging from '0x00' to '0x0F'. The Record number is a 1-byte value ranging from '0x01' to '0xFF'.

If the selected device type is **SCSI**, **NVMe**, **Tape**, or **ECKD** and IPL type **CCW** is selected, this field is unavailable.

Worldwide port name:

Specify the Worldwide Port Number identifying the Fibre Channel port of the SCSI target device (according to the FCP/SCSI-3 specifications). This is a 64-bit binary number designating the port name, represented by 16 hexadecimal digits. This is required for SCSI load or SCSI dump.

If the selected device type is **ECKD**, **NVMe** or **Tape**, this field is unavailable.

Logical unit number:

Specify the number of the logical unit as defined by FCP (according to the FCP/SCSI-3 specifications). This is the 64-bit binary number designating the unit number of the FCP I/O device, represented by 16 hexadecimal digits. This field is required for SCSI load or SCSI dump.

If the selected device type is **ECKD**, **NVMe**, or **Tape**, this field is unavailable.

Boot program selector:

This field identifies the program to load from the FCP-load device and contains a decimal value in the range from 0 to 30. This parameter provides the possibility of having up to 31 different boot configurations on a single disk device. This field should be set to 0 for optical media SCSI devices.

If the selected device type is **Tape** or **ECKD** and IPL type **CCW** is selected, this field is unavailable.

Boot record logical block address:

Specify the load block address if your file system supports dual-boot or booting from one of the multiple partitions. If no block address is specified, the logical-block address of the boot record is assumed to be zero. This feature could be used to IPL using a second or backup boot record, in case the original one is corrupted or overwritten by accident.

This field is unavailable if a device type of **ECKD** or **Tape** are selected.

Operating system load parameters:

Specify a variable number of characters to be used by the program that is loaded. This information will be given to the IPLed operating system and will be ignored by the machine loader. The IPLed operating system (or standalone dump program) has to support this feature. Any line breaks you enter are transformed into spaces before being saved.

If the selected device type is **Tape** or **ECKD** and IPL type **CCW** is selected, this field is unavailable.

Image pages

This window displays an activation profile for activating a logical partition as an image. The window displays the image name.

Make a selection from the Profile Tree to view the image pages in the profile:

General
To describe the image profile and its purpose, and to identify the operating mode established for the logical partition activated by the profile, select **General**.

Processor
To customize information that assigns logical processors to the logical partition activated by the profile, select **Processor**.

Security
To customize settings that determine the extent of interaction between the logical partition activated by the profile and other logical partitions activated on the same CPC, click **Security**.

Storage
To set the amount of storage assigned to the logical partition activated by the profile, select **Storage**.

Options
To specify the image option for the processor values, select **Options**.

Load
To customize information that controls loading a control program for the logical partition activated by the profile, select **Load**.

Note: Not available when Coupling facility or Secure Service Container are selected on the **General** image page.

“SSC” on page 534
To set up the IBM Secure Service Container (Secure Service Container), select **SSC**.

Crypto
To customize information that controls how the logical partition activated by the profile uses coprocessors and accelerators assigned to it, select **Crypto**.

Note: Not available when Coupling facility is selected on the **General** image page.

Time Offset
To set the logical partition's clock using an offset from the External Time Source's time of day, select **Time Offset**.

Note: Available when **Logical partition offset** is selected on the **General** image page.

General

Use this window to describe the image profile and its purpose and to identify the operating mode established for the logical partition activated by the profile.

Profile name

Specify the name of the profile you want to work with:

- To customize a new profile, enter a new name in the field.
- To view or customize an existing profile, select the arrow beside the field to list the names of existing profiles. Then select a profile name from the list to display its information.

A profile name is required to save the information.

A profile name can be from 1 to 8 characters long. It cannot have special characters or imbedded blanks. Valid characters for a profile name are:

Characters 0 through 9
Decimal digits

Characters A through Z
Letters of the English alphabet

Note: Profile names are not case-sensitive. All alphabetic characters are saved in uppercase.

Description

Specify a brief note, up to 50 characters long, that describes the contents or purpose of the profile.

Note: A description is recommended, but optional.

Partition identifier

Specify the two hexadecimal digits partition identifier to be used by the logical partition. The partition identifier can be from X'0' to X'7F' or X'0' to X'3F' (Hardware Management Console Version 2.12.1 and earlier).

The partition identifier must also be unique among the identifiers of other logical partitions activated by the reset profile. If necessary, check the partition identifier fields on the other **General** image pages to verify the partition identifier assigned to this image is unique.

Mode

Select the operating mode to establish during activation to support the type of control program that can operate on the logical partition.

The mode determines some of the other types of information included in the image profile. Different profile information is associated with each different mode.

Note: Changing mode discards information exclusively associated with it. For example, changing from any mode to coupling facility mode discards the profile page that contains the load information and the profile page that contains the crypto information.

Clock Type Assignment

Select a time source for setting the logical partition's time-of-day (TOD) clock.

The logical partition's clock is synchronized with the central processor complex time-of-day clock (CPC TOD clock). Ordinarily, the logical partition's clock is set to the same time as the CPC's time source (either the CPC TOD clock or an external time reference, such as a Server Time Protocol(STP). You can use this group box to select another source for setting the logical partition's clock.

Standard time of day
To set the logical partition's clock to the same time set for the CPC's time source (either the CPC TOD clock or an external time reference, such as the Server Time Protocol (STP), select **Standard time of day**.

Logical partition time offset
If the CPC uses a Sysplex Timer as its time source, select **Logical partition time offset** to set the logical partition's clock using an offset from the External Time Source's time of day. Then use the **Time Offset** window to set the offset.

Ensure that the image profile data conforms to the current maximum LICCC configuration

Select this option to ensure that the image profile data conforms to the current maximum Licensed Internal Code Configuration Control (LICCC) configuration. The data entered in the image profiles has to be compatible and supported by the LICCC. If image profile data changes, is imported, or the LICCC definition changes the profiles will be modified automatically to meet the new LICCC configuration. If this option is unchecked, the data entered for an image profile can be outside the valid LICCC configuration.

Note: It is recommended that image profile data conform to the current maximum LICCC configuration.

Processor

Use this window to customize information that determines the allocation and management of processor resources assigned to the logical partition activated by the profile.

Use the **Logical processor assignment** group box to customize the logical partition's logical processor assignment.

Note: The **Mode** list on the **General** image page lists the operating modes. The logical partition operates in the selected mode upon being activated with this profile. Depending on the selected mode and what processors are installed in your system will determine the allocation and management of the processor resources.

You can find more detailed help on the following elements of this window:

Group Name

To change the group profile name assigned to the logical partition, select the arrow beside the field to list the names of existing group profiles and select a new group or create your own group profile name. A logical partition can be assigned to only one group.

Note: If the group profile name is blank, then the logical partition is not assigned to a group.

Logical Processor Assignment (CPs - General and SSC modes)

Use these selections to customize the logical partition's logical processor assignment.

Make a selection to choose the physical processors you want assigned to the logical partition's logical processors. Your selection determines which controls you need to use to complete customizing the logical processor assignment.

Dedicated central processors
If you want a central processor dedicated to each logical processor, select **Dedicated central processors**

Not dedicated central processors
If you want the logical processors to share *not dedicated central processors* (central processors that are not already dedicated to other activated logical partitions when this logical partition is activated), select **Not dedicated central processors**

Logical Processor Assignment (CPs/zIIPs - General mode)

Use these selections to customize the logical partition's logical processor assignment.

Make a selection to choose the physical processors you want assigned to the logical partition's logical processors. Enter the initial and reserved number of processors for your selection. Your selection determines which controls you need to use to complete customizing the logical processor assignment.

Notes:

1. If you have temporary processors that are installed for use on your system, you can specify an initial number of processors that does not exceed the number of physical processors configured plus the number of installed temporary processors even if the temporary processors are not currently

activated. You will not be able to activate the image unless the temporary processors are activated or the LICCC has been permanently updated to include extra processors.

2. Unless you plan to have your LICCC updated, it is best to specify the number of initial processors that does not exceed the number of configured physical processors and specify the temporary processors as reserved. The image can be activated without having to activate the temporary processors. The reserved processors can be brought on-line after the temporary processors have been activated and configured off-line before deactivating the temporary processors.
3. If you have temporary processors of a given type, but no physical processors of the same type, you can specify up the number of temporary processors of that type. You will not be able to activate it unless the temporary processors are activated or until the LICCC has been permanently updated to include the new processor types.

Dedicated central processors
If you want a central processor dedicated to each logical processor, select **Dedicated processors**.

Dedicated z Integrated Information Processors (zIIPs)
If z Integrated Information Processors (zIIPs) is supported by and installed in the Central Processor Complex (CPC), select **Dedicated processors**, then select **z integrated information processors** if you want to assign zIIPs to each logical processor.

Not dedicated central processors
If you want the logical processors to share *not dedicated central processors* (central processors that are not already dedicated to other activated logical partitions when this logical partition is activated), select **Central processors**.

Not dedicated z Integrated Information Processors (zIIPs)
If z Integrated Information Processors (zIIP) are supported by and installed in the Central Processor Complex (CPC), select **z Integrated Information Processors** to assign not dedicated zIIPs that are not already dedicated to other activated logical partitions when this logical partition is activated).

Logical Processor Assignment (CPs/ICFs - Coupling facility mode)

Use these selections to customize the logical partition's logical processor assignment.

Make a selection to choose the physical processors you want assigned to the partition's logical processors. Your selection determines which controls you need to use to complete customizing the logical processor assignment.

Dedicated central processors
If you want a central processor dedicated to each logical processor, select **Dedicated central processors**.

Dedicated internal coupling facility processors
If internal coupling facility processors are supported by and installed in the central processor complex (CPC), select **Dedicated internal coupling facility processors** if you want one dedicated to each logical processor.

Not dedicated central processors
If you want the logical processors to share *not dedicated central processors* (central processors that are not already dedicated to other activated logical partitions when this logical partition is activated), select **Not dedicated central processors**.

Not dedicated internal coupling facility processors
If you want the logical processors to share *not dedicated internal coupling facility processors* (internal coupling facility processors that are not already dedicated to other activated logical partitions when this logical partition is activated), select **Not dedicated internal coupling facility processors**.

Not dedicated internal coupling facility processors and not dedicated central processors
If internal coupling facility processors are supported by and installed in the central processor complex (CPC), select **Dedicated internal coupling facility processors and not dedicated central processors** if you want to assign a combination of dedicated internal coupling facility processors *and* not dedicated central processors to the logical partition.

Note: This option is only available on the console for Version 2.10.2 and earlier.

Dedicated and not dedicated internal coupling facility processors
If internal coupling facility processors are supported by and installed in the CPC, select **Dedicated and not dedicated internal coupling facility processors and not dedicated central processors** if you want to assign a combination of dedicated internal coupling facility processors *and* not dedicated internal coupling facility processors to the logical partition.

Note: This option is only available on the console for Version 2.10.2 and earlier.

Logical Processor Assignment (CPs/IFLs - Linux only mode)

Use these selections to customize the logical partition's logical processor assignment.

Make a selection to choose the physical processors you want assigned to the logical partition's logical processors. Your selection determines which controls you need to use to complete customizing the logical processor assignment.

Dedicated central processors
If you want a central processor dedicated to each logical processor, select **Dedicated central processors**.

Dedicated Integrated Facilities for Linux
If Integrated Facilities for Linux (IFL) is supported and installed in the Central Processor Complex (CPC), select **Dedicated Integrated Facilities for Linux** if you want an integrated facilities for Linux dedicated to each logical processor.

Not dedicated central processors
If you want the logical processors to share *not dedicated central processors* (central processors that are not already dedicated to other activated logical partitions when this logical partition is activated), select **Not dedicated central processors**.

Not dedicated Integrated Facility for Linux
If you want the logical processors to share *Not dedicated integrated facilities for Linux* (integrated facilities for Linux processors that are not already dedicated to other activated logical partitions when this logical partition is activated), select **Not dedicated Integrated Facilities for Linux (IFLs)**.

Logical Processor Assignment (CPs/zAAPs/zIIPs/ICFs/IFLs - z/VM mode)

Use these selections to customize the logical partition's logical processor assignment.

Make a selection to choose the physical processors you want assigned to the logical partition's logical processors. Enter the initial and reserved number of processors for your selection. Your selection determines which controls you need to use to complete customizing the logical processor assignment.

Notes:

1. If you have temporary processors that are installed for use on your system, you can specify an initial number of processors that does not exceed the number of physical processors configured plus the number of installed temporary processors even if the temporary processors are not currently activated. You will not be able to activate the image unless the temporary processors are activated or the LICCC has been permanently updated to include extra processors.
2. Unless you plan to have your LICCC updated, it is best to specify the number of initial processors that does not exceed the number of configured physical processors and specify the temporary processors as reserved. The image can be activated without having to activate the temporary processors. The reserved processors can be brought on-line after the temporary processors have been activated and configured off-line before deactivating the temporary processors.
3. If you have temporary processors of a given type, but no physical processors of the same type, you can specify up the number of temporary processors of that type. You will not be able to activate it unless the temporary processors are activated or until the LICCC has been permanently updated to include the new processor types.

Dedicated central processors
If you want a central processor dedicated to each logical processor, select **Dedicated processors**.

Dedicated z Integrated Information Processors (zIIPs)
If z Integrated Information Processors (zIIPs) is supported by and installed in the central processor complex (CPC), select **Dedicated processors**, then select **z Integrated Information Processors** if you want to assign zIIPs to each logical processor.

Dedicated Internal Coupling Facility Processors
If internal coupling facility is supported by and installed in the central processor complex (CPC), select **Dedicated processors**, then select **Internal Coupling Facility Processors (ICFs)** if you want to assign *internal coupling facility processors* to each logical processor.

Dedicated Integrated Facilities for Linux
If integrated facilities for Linux is supported by and installed in the central processor complex (CPC), select **Dedicated processors**, then select **Integrated Facilities for Linux (IFLs)** if you want to assign *Integrated Facilities for Linux* to each logical processor.

Not dedicated central processors
If you want the logical processors to share *not dedicated central processors* (central processors that are not already dedicated to other activated logical partitions when this logical partition is activated), select **Central processors**.

Not dedicated z Integrated Information Processors (zIIPs)
If z Integrated Information Processors (zIIPs) are supported by and installed in the central processor complex (CPC), select **z Integrated Information Processors** to assign not dedicated zIIPs (zIIPs that are not already dedicated to other activated logical partitions when this logical partition is activated).

Not dedicated Internal Coupling Facility Processors
f internal coupling facility processors are supported by and installed in the central processor complex (CPC), select **Internal Coupling Facility Processors (ICFs)** to assign not dedicated internal coupling facility processors (internal coupling facility processors that are not already dedicated to other activated logical partitions when this logical partition is activated).

Not dedicated Integrated Facilities for Linux
If Integrated Facilities for Linux are supported by and installed in the Central Processor Complex (CPC), select **Integrated Facilities for Linux (IFLs)** to assign not dedicated integrated facilities for Linux (integrated facilities for Linux processors that are not already dedicated to other activated logical partitions when this logical partition is activated).

Processor type (General, z/VM, and Coupling facility modes)

This field represents the number of processors that are used each time you activate a partition.

A *logical processor* is the processor resource defined to operate in a logical partition as a physical processor. A logical partition's control program uses its logical processors to perform jobs for the logical partition.

Initial
Specify the number of logical processors to assign to the logical partition.

The number of processors can be from one to the maximum number of physical processors available to the logical partition. The maximum number of processors available is limited by:

- The number of physical processors configured and available.
- The number of processors supported by the operating mode selected on the **General** image page.
- The number of processors that are not already dedicated to another active logical partition at the time of the next activation.
- The number of processors supported by the control program at the time of the next activation.

Reserved
Specify the number of reserved processors available that you want assigned to the logical partition.

Reserved processors can be configured online at a later time. Reserved processors can be defined at partition activation time, but are not used during partition activation. Instead, they are configured offline during activation automatically, and can be manually configured online. The reserved processor

may or may not be available when the system is activated. If it is not available when the system is activated, it can become available during concurrent upgrade.

The ability to add and remove dedicated processors does not require deactivating/activating the partitions. This support is not restricted to concurrent upgrade purposes.

Not Dedicated Processor Details (General, Coupling facility, Linux only, z/VM, and SSC modes)

Use this section to specify initial processing weight, minimum and maximum processing weight, select whether or not to enable initial capping and workload manager, and to specify absolute capping.

Initial processing weight

Specify the logical partition's processing weight for sharing the not dedicated processors.

The *not dedicated* processors are processors not already dedicated to other activated logical partitions when this logical partition is activated. This logical partition's *processing weight* is its share of the not dedicated processors. The processing weight can be from 1 to 999.

The exact percentage of the not dedicated processors allocated to the logical partition depends upon the processing weights of other logical partitions defined and activated on the same Central Processor Complex (CPC). That percentage is calculated by dividing the logical partition processing weight by the sum of the processing weights of all active logical partitions on the CPC.

A processing weight is a target, not a limit. It represents the share of the not dedicated processor resources guaranteed to a logical partition when all the resources are in use. When resources are available, this logical partition can borrow them if necessary. When this logical partition is not using its share of the resources, other logical partitions can use those resources.

Notes:

1. While excess resources are available, processing weights have no effect on how those resources are used. Weights take effect when the number of logical processors requiring a timeslice is greater than the number of not central processors.
2. This field is available only when either of the following selections are made:
   - **Not dedicated central processors**
   - **Not dedicated internal coupling facility processors**
   - **Dedicated internal coupling facility processors and not dedicated central processors**

     Note: This option is only available on the console for Version 2.10.2 and earlier.
   - **Not dedicated integrated facility for Linux**
   - **Not dedicated z Integrated Information Processors (zIIPs)**

   Otherwise, this field is unavailable.

Initial capping

You can specify whether the logical partition is prevented from using the not dedicated processors in excess of its processing weight.

To indicate the logical partition *cannot* use the not dedicated processors in excess of its processing weight, select **Initial capping**. That is, the processing weight is capped.

Otherwise, it indicates it can use the not dedicated processors in excess of its processing weight when the resources are not in use by another logical partition. That is, the processing weight is not capped.

The *Not dedicated processors* are processors not already dedicated to other activated logical partitions when this logical partition is activated. This logical partition's *processing weight* is its share of the not dedicated processors. Ordinarily, a processing weight is a target, not a limit. When the processing weight is *capped*, it is a limit.

Notes:

1. If this logical partition's share of the not dedicated processors is capped, it does not affect the shares set for other activated logical partitions.
2. This field is available only when the **Enable workload manager** check box is not checked and either of the following selections are made:
   - **Not dedicated central processors**
   - **Not dedicated integrated coupling facility processors**
   - **Dedicated integrated coupling facility processors and not dedicated central processors**

     Note: This option is only available on the console for Version 2.10.2 and earlier.
   - **Dedicated and not dedicated internal coupling facility processors**

     Note: This option is only available on the console for Version 2.10.2 and earlier.
   - **Not dedicated Integrated Facility for Linux**
   - **Not dedicated z Integrated Information Processors (zIIPs)**. Otherwise, this field is unavailable.

Enable workload manager

You can select either **Enable workload manager** or **Initial capping**, but not both. However, you do not have to select either one.

To enable the Workload Manager Intelligent Resource (IRD) weight management function, select **Enable workload manager**. Selecting WLM from one processor details automatically selects WLM from the other processor details and conversely. Specify the minimum and maximum processing weights. Changes to LPAR management weights based on customer Workload Management policies and current work loads. For more information, refer to *z/OS MVS Planning: Workload Management* for the release of z/OS that you are using.

Minimum processing weight
Minimum processing weight is the lowest weight that IRD weight management can use. The value must be less than or equal to the initial processing weight.

Maximum processing weight
Maximum processing weight is the highest weight that IRD weight management can use. Maximum processing weight must be greater than or equal to the initial processing weight.

Note: This field is available only when the **Initial capping** check box is not checked for any of the processor types and either of the following selections are made:

- **Not dedicated integrated facility for Linux**
- **Not dedicated central processors**
- **Not dedicated z Integrated Information Processors (zIIPs)**

Otherwise, this field is unavailable.

Absolute Capping

You can specify whether the logical partition can use the not dedicated processors absolute capping.

To indicate the logical partition *can* use the not dedicated processors absolute capping, select **Absolute capping** to specify an absolute number of processors to cap the logical partition's activity. The absolute capping value can either be None or a number of processors value from 0.01 to 255.0 can be specified.

Otherwise, it indicates the logical partition *cannot* use the not dedicated processors absolute capping when the resources are in use by another logical partition. That is, the processing absolute number is not capped.

The *Not dedicated processors* are processors not already dedicated to other activated logical partitions when this logical partition is activated. This logical partition's *absolute capping* is its share of the not dedicated processors. When the absolute processing number is *capped*, it is a limit.

Notes:

1. If this logical partition's share of the not dedicated processors is capped, it does not affect the shares set for other activated logical partitions.
2. This field is available only when either of the following selections are made:
   - **Not dedicated central processors**
   - **Not dedicated integrated coupling facility processors**
   - **Not dedicated integrated facility for Linux**
   - **Central processors**
   - **Not dedicated z Integrated Information Processors (zIIPs)**

   Otherwise, this field is unavailable.

Security

Use this window to customize settings that determine the extent of interaction between the logical partition activated by the profile and other logical partitions activated on the same Central Processor Complex (CPC).

Partition Security Options

Use this section to specify the security options for the logical partitions activated by the profile.

Global performance data control
To indicate whether the logical partition can be used to view the processing unit activity data for all other logical partitions activated on the same CPC, select **Global performance data control**.

Input/output (I/O) configuration control

To indicate whether the logical partition can be used to read and write any Input/Output Configuration Data Set (IOCDS) in the configuration, select **Input/Output (I/O) configuration control**.

Selecting this option indicates the logical partition can also be used to change the input/output (I/O) configuration dynamically and controls whether or not a logical partition can enter config mode.

Additionally, this control allows the OSA Support Facility to control OSA configuration for other LPs and allows access to certain STP data.

Cross partition authority
To indicate whether the logical partition can be used to issue control program instructions that reset or deactivate other logical partitions, select **Cross partition authority**.

Logical partition isolation

To indicate whether reconfigurable channel paths assigned to the logical partition are reserved for its exclusive use, select **Logical partition isolation**.

When selected, channel paths are configured off; they will not become available to other logical partitions.

When not selected, reconfigurable channel paths assigned to this logical partition are not reserved for its exclusive use. Its channel paths can be configured off and reassigned to other logical partitions.

BCPii Permissions

Use this section to enable the Base Control Program internal interface (BCPii) permissions for the selected logical partition activated by the profile.

Enable the partition to send commands
To enable the selected partition to send BCPii commands, select **Enable the partition to send commands**. When selected, the active logical partition can send BCPii commands to other active logical partitions.

Enable the partition to receive commands from other partitions
To enable the selected partition to receive BCPii commands from other partitions, select **Enable the partition to receive commands from other partitions**. When selected, the active logical partition can receive BCPii commands from other active logical partitions.

All partitions
Select this option if you want the selected logical partition to receive BCPii commands from all the active logical partitions.

"Add partition" on page 532 (Selected partitions)
Select this option if you want to remove or add selected logical partitions to receive BCPii commands from the logical partition.

Add
To add a system and logical partition to receive BCPii commands from the logical partition, click **Add**.

Remove
To remove a selected logical partition to receive BCPii commands from the logical partition, click **Remove**.

Counter Facility Security Options

Use this section to specify the counter facility security options for the logical partitions activated by the profile.

Basic counter set authorization control
To indicate whether authorization is allowed to use the basic counter set, select **Basic counter set authorization control**. The set can be used in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is running.

Problem state counter set authorization control
To indicate whether authorization is allowed to use the problem-state counter set, select **Problem state counter set authorization control**. The set can be used in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is in problem state.

Crypto activity set authorization control
To indicate whether authorization is allowed to use the crypto-activity counter set, select **Crypto activity counter set authorization control**. The set can be used to identify the crypto activities contributed by the logical CPU and the blocking effects on the logical CPU.

Extended counter set authorization control
To indicate whether authorization is allowed to use the extended counter set, select **Extended counter set authorization control**. The counters of this set are model dependent.

Sampling Facility Security Options

Use this section to specify the sampling facility security options for the logical partitions activated by the profile.

Basic sampling authorization control
To indicate whether authorization is allowed to use the basic-sampling function, select **Basic sampling authorization control**. The sample data includes an instruction address, the primary ASN, and some state information about the CPU. This allows tooling programs to map instruction addresses into modules or tasks, and facilitates determination of hot spots.

Diagnostic sampling authorization control

Note: This option is available if the **Basic sampling authorization control** option has been selected. However, if this option is selected the **Basic sampling authorization control** option cannot be deselected.

To indicate whether authorization is allowed to use the diagnostic-sampling function, select **Diagnostic sampling authorization control**. The sample data includes an instruction address, the

primary ASN, and some state information about the CPU. This allows tooling programs to map instruction addresses into modules or tasks, and facilitates determination of hot spots.

CP Assist for Cryptographic Functions

Use this section to specify the CP Assist Cryptographic Functions (CPACF) for the logical partitions activated by the profile.

Note: The default setting is to permit.

Permit AES key import functions

To change the current Advanced Encryption Standard (AES) key import functions setting for CPACF when the logical partition is activated, select **Permit AES key import functions**.

Permit DEA key import functions

To change the current Data Encryption Algorithm (DEA) key import functions setting for CPACF when the logical partition is activated, select **Permit DEA import key functions**.

Permit ECC key import functions

To change the current Elliptical Curve Cryptography (ECC) key import functions setting for CPACF when the logical partition is activated, select **Permit ECC import key functions**.

Add partition

Use this window to specify the partitions from which the target partition can receive BCPii commands.

Enter system and partition manually

System: Enter the system name for the logical partition from which the target partition can receive BCPii commands.

Netid: Enter the Netid name for the selected system.

Partition: Enter the logical partition name from which the target partition can receive BCPii commands.

Select a system and partition

System: Select from the drop-down menu the system for the logical partition from which the target partition can receive BCPii commands.

Netid: The Netid displays for the selected system.

Partition: Select from the drop-down menu the active logical partition from which the target partition can receive BCPii commands.

Additional functions on this window include:

Add

To add a selected system and partitions, click **Add**.

Cancel

To exit the current window without saving changes, click **Cancel**.

Help

To display help for the current window, click **Help**.

Storage

Use this window to set the amount of central storage and virtual flash memory assigned to the logical partition activated by the profile.

Central Storage

Use this section to customize information that determines the amount and starting position of central storage allocated to the logical partition.

Amount in:
Displays the amount of storage is that is installed in the selected partition. Use the down arrow to change the amount of storage in Gigabytes, Megabytes, or Terabytes.

Initial
Enter the amount of central storage to allocate to the logical partition upon activation.

Initial storage is allocated to a logical partition in a contiguous block of one Gigabyte (GB) units. The logical partition has exclusive use of its initial storage. That is, it is not shared with other active logical partitions.

You must allocate at least 1 GB of initial storage for all operating modes.

Reserved
Enter the amount of central storage that can be reconfigured dynamically to the logical partition after activation. This field is only active if the operating mode selected on the **General** image page is **General**, **LINUX only**, or **z/VM** mode. It is not available in coupling facility mode.

Reserved storage is allocated to a logical partition in a contiguous block of one Gigabyte (GB) units, and is contiguous to an located above its initial storage. But, unlike its initial storage, the logical partition does not have exclusive use of its reserved storage. The reserved storage provides the logical partition with an additional amount of storage to use only if it is not already being used by another active logical partition.

There is no minimum for reserved storage. Zero gigabytes (0 GB) is a valid amount of reserved storage.

Storage origin
Use these selections to indicate how the central storage origin is determined.

The central storage origin of a logical partition is the storage location from which its central storage allocation begins. The origin can be any location that provides sufficient, contiguous space for allocating the total central storage for the logical partition.

Determined by the system
To have the Central Processor Complex (CPC) determine the central storage origin, select **Determined by the system**.

The CPC allocates central storage, wherever sufficient, contiguous space is available.

Determined by the user
To have this profile set the central storage origin, select **Determined by the user**, then specify the origin in the **Origin** field.

Origin
If you select to have this profile set the central storage origin, enter the origin here. The origin is an offset, not an address. Enter the offset number from where available CPC central storage begins, to where you want logical partition central storage to begin.

When this profile is used to activate a logical partition, sufficient and contiguous space must be available from the origin for the amount of central storage specified. Logical partition activation fails if sufficient storage is not available from the origin, regardless of whether the origin is determined by the system or by the user through this profile.

Virtual Flash Memory

Use these selections to customize information that determines the amount and virtual flash memory storage allocated to the logical partition. The virtual memory increments in 16 GB amounts with a maximum of 6144 GB. This field is only active if the operating mode selected on the **General** image page is **General**, **LINUX only**, or **z/VM** mode. It is not available in coupling facility mode.

Initial
Use the number spinner to increment or decrement the initial amount of virtual flash memory for the selected partition in 16 GB increments.

Maximum
Use the number spinner to increment or decrement the maximum amount of virtual flash memory to a allow for the selected partition.

View Storage Information
Select the View Storage Information link to open the **Storage Information** task. You can view the virtual flash memory storage allocation for the selected partition.

Options

Specify the image options for the processor values on this window:

Minimum and Maximum I/O priority values can be specified at a partition level. These minimum and maximum I/O priority values can both be set at partition activation time or dynamically (post partition activation).

Minimum I/O priority

The minimum value must be less than or equal to the maximum value entered. This value can range from 0 to the maximum I/O priority allowed for that processor.

The minimum default is a priority value of 0.

Maximum I/O priority

This maximum processor I/O priority is obtained from new System Information support.

The maximum default is a priority value of 0.

Defined capacity
The measure of processor resource consumption for a logical partition, expressed in millions of service units (MSU) per hour.

CP management cluster name
The name specified for the CP management cluster.

SSC

Use this window to customize IBM Secure Service Container (Secure Service Container) configuration settings for the selected logical partition in Secure Service Container mode.

Note: Cryptographic (Crypto) options can be selected for Secure Service Container partitions.

The Secure Service Container configuration settings include the following:

Boot selection
Before a Secure Service Container partition is restarted for the first time, all fields of activation profiles can be updated or saved.

Secure Service Container installer
This option is selected until the Secure Service Container partition is restarted and the input fields contain information that was previously defined.

Secure Service Container
This option is selected after the Secure Service Container partition is restarted. The **Reset Logon Settings** and **Reset Network Settings** can be updated after the restart.

Reset Logon Settings
To reset the logon settings after the Secure Service Container partition is restarted, click **Reset Logon Settings**. Click **Yes** to proceed with resetting the master logon settings, then provide new information in the logon input fields.

Note: The input areas are pre-filled with the old settings.

Reset Network Settings
To reset the network settings after the Secure Service Container partition is restarted, click **Reset Network Settings**. Click **Yes** to proceed with resetting the master logon settings, then provide new information in the network input fields.

Note: The input areas are predefined with the old settings.

Master user ID
Use this field to specify the master user ID for the selected Secure Service Container logical partition.

A master user ID can be from one to 32 characters long. It cannot have special characters or embedded blanks. Valid characters for a master user ID name are numbers **0** through **9**, alphabetic, period, underscores, and minus symbol.

Master password
Use this field to specify the master password for the master user ID you specified.

A master password can have a minimum of 8 characters and a maximum of 256 characters.

Confirm master password
Use this field to specify again the same master password you specified in the **Master password** field.

Host name
Use this field to specify the host name for the selected Secure Service Container logical partition.

A host name can be from one to 32 characters long. It cannot have special characters or embedded blanks. Valid characters for a host name are alphanumeric characters, periods (.), colons (:), and hyphens (-).

IPv4 gateway
Use this field to specify the default gateway IPv4 address.

IPv6 gateway
Use this field to specify the default gateway IPv6 address.

Network Adapters

Use the Network Adapter table to view and change an IP address type and detail settings for the selected network adapters. You can add, edit, or remove the IP address type and detail settings using the **Select Action** list from the table tool bar. A maximum of 100 network adapters can be specified.

CHPID
Displays the CHPID for the selected Secure Service Container logical partition.

VLAN
Displays the VLAN for the selected Secure Service Container logical partition.

Port
Displays the Port 0/1 parameter for the selected Secure Service Container logical partition.

IP address
Displays the IPv4 or IPv6 address for the selected Secure Service Container logical partition. Also, indicates DHCP or Link Local if that is the specific IP address type.

Mask/Prefix
Displays the Mask/Prefix for the IPv4 or IPv6 address specified.

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Add...
Select this operation to add a new IP address type and CHPID/VLAN details for the selected Secure Service Container logical partition.

Edit...
Select this operation to edit the selected IP address type and CHPID/VLAN details for the selected Secure Service Container logical partition.

Delete
Select this operation to delete the selected IP address type and CHPID/VLAN details for the selected Secure Service Container logical partition.

The icons perform the following functions in the Network Adapters table:

Show Filter Row
Displays a row under the title row of the table.

Clear All Filters
Returns to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table.

Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Configure Columns
Selects which columns you want to display. Arrange the columns in the table in the order you want or hide columns from view. All available columns are displayed in the **Columns** list by their column name. You select the columns you want to display or hide by selecting or clearing the items in the list and using the arrows to the right of the list to change the order of the selected column. When you have completed the configuration, click **OK**. The columns are displayed in the table as you specified. Your configuration changes are saved and reloaded the next time that you launch this task.

DNS Servers

The DNS Servers table displays the IPv4 or IPv6 address for the selected Secure Service Container logical partition. You can add, edit, or remove the IP address using the **Select Action** list from the table tool bar. A maximum of 2 DNS addresses can be specified.

DNS is a distributed database system for managing host names and their associated Internet Protocol (IP) addresses. Using DNS means that people can use names, such as "www.jkltoys.com" to locate a host, rather than using the IP address (xxx.xxx.xxx.xxx). A single server may only be responsible for knowing the host names and IP addresses for a small subset of a zone, but DNS servers can work together to map all host names to their IP addresses. DNS servers working together allow computers to communicate across the Internet.

IP address
Displays the current IPv4 or IPv6 address for the selected Secure Service Container logical partition.

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Add...
Select this operation to add a new IPv4 or IPv6 address to the selected Secure Service Container logical partition.

Edit...
Select this operation to edit the selected IPv4 or IPv6 address specified for the selected Secure Service Container logical partition.

Remove
Select this operation to remove the selected IPv4 or IPv6 address for the selected logical partition.

The icons perform the following functions in the DNS Servers table:

Show Filter Row
Displays a row under the title row of the table.

Clear All Filters
Returns to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table.

Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Add/Edit Network Adapters Entry

Use this window to add or edit the CHPID, VLAN, or Port for the selected secure service container logical partition. If the IP address selected is a static IPv4 or IPv6, you can edit or add the corresponding IP address.

OK
To perform the selected operation, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add/Edit DNS Entry

Use this window to add or edit the static IPv4 or IPv6 address configured for the selected secure service container logical partition.

OK
To perform the selected operation, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Load

Use this window to customize information that controls loading a control program for the logical partition activated by the profile.

Note: The image pages do not include this additional page if the operating mode selected on the **General** image page is Coupling facility or SSC mode.

Load during activation

To indicate whether the load is performed during activation, select **Load during activation**.

If it has been selected it indicates a load is performed. The other information on the window is used to perform the load. Otherwise, a load is not performed.

Device type
Select the type of device to perform a load for the logical partition. You would use the SCSI or NVMe option to do a standalone dump to a SCSI device or NVMe adapter.

ECKD
To perform an IPL on the logical partition from ECKD DASD device type, click **ECKD**. Optionally, clear main storage on the logical partition before loading.

SCSI
To perform an IPL on the logical partition from SCSI device type, click **SCSI**.

NVMe
To perform an IPL on the logical partition from NVMe device type, click **NVMe**.

Tape
To perform an IPL on the logical partition from Tape device type, click **Tape**. Optionally, clear main storage on the logical partition before loading.

IPL type:
Select the type of IPL for the selected **ECKD** device type to perform for the logical partition.

Channel Command Word (CCW)
To perform the load on CCW IPL, click **Channel Command Word (CCW)**.

List-directed
To perform the load on a list-directed IPL, click **List-directed**.

If the selected device type is **SCSI**, **NVMe**, or **Tape** this field is unavailable.

Load type:
Select the type of load to perform for the logical partition. You would use the SCSI or NVMe option to do a standalone dump to a SCSI device or NVMe adapter.

Load an OS
To perform an operating system load type on the logical partition, click **Load an OS**.

Load a dump program
To perform a dump program load type on the logical partition, click **Load a dump program**.

Validation:

Enable Secure Boot
To verify the signature of the load program and distributor's signature match, select **Enable Secure Boot**.

Certificates
The Certificates table displays the imported certificates assigned to the partitions.

If the selected device type is **Tape** or **ECKD** and IPL type **CCW** is selected this field is unavailable.

Load address:

Enter the address of the input/output (I/O) device that provides access to the control program to load. For a SCSI load or NVMe load, this field has the device number of the device (for example, fibre channel adapter) that is used to perform the SCSI or NVMe load. This should contain four hexadecimal digits for NVMe load or five hexadecimal digits for SCSI load.

A load address is required.

The source of the control program must be an I/O device in the I/O configuration that is active when this profile is activated. The I/O device can store the control program or can be used to read the control program from a data storage medium.

Note: This field is applicable only when **Use dynamically changed address** check box is empty. Otherwise, if the check box displays a check mark, this field is unavailable.

Use dynamically changed address

To indicate whether the load address is dynamically determined by changes to the channel subsystem Input/Output definition (I/O), select **Use dynamically changed address**.

If this is selected, the load address is dynamically determined. Otherwise, this profile sets the load address. See the **Load address** field for the address set by this profile.

Specify the address in the **Load address** field.

Load parameter:

Specify the optional information, if any, to use to further control how the control program is loaded during activation. Valid characters for a load parameter are:

- At (@)
- Pound (#)

- Dollar ($)
- Blank character
- Period (.)
- Decimal digits 0 through 9
- Capital letters A through Z .

Some control programs support the use of a load parameter to provide additional control over the performance or outcome of a load. Check the configuration programming and reference documentation for the control program to determine the load parameters that are available and their effects on a load.

Note: This field is applicable only when **Use dynamically changed parameter** is **not** selected. Otherwise, this field is unavailable.

Use dynamically changed parameter

To indicate whether the load parameter is dynamically determined by changes to the channel subsystem Input/Output (I/O) definition, select **Use dynamically changed parameter**

If this is selected, the load parameter is dynamically determined. Otherwise, this profile sets the load parameter. Enter the parameter for this profile in the **Load parameter** field.

Time-out value:

Specify the amount of time to allow for the completion of the load.

The time-out value can be from 60 to 600 seconds. If the load operation cannot be completed within the specified time, the operation is canceled.

If the selected device type is **SCSI**, **NVMe**, or **ECKD** and IPL type **List-directed** is selected, this field is unavailable.

Boot record location:

The boot record location (C,H,R format) parameters can be specified from the volume label or be specified.

- Select **use volume label** to specify the boot record label from the volume label
- Select to specify the C,H,R format. The Cylinder number is a 4-byte value ranging from '0x00000000' to '0x0FFFFFFF'. The Head number is a 1-byte value ranging from '0x00' to '0x0F'. The Record number is a 1-byte value ranging from '0x01' to '0xFF'.

If the selected device type is **SCSI**, **NVMe**, **Tape**, or **ECKD** and IPL type **CCW** is selected, this field is unavailable.

Worldwide port name:

Specify the Worldwide Port Number identifying the Fibre Channel port of the SCSI target device (according to the FCP/SCSI-3 specifications). This is a 64-bit binary number designating the port name, represented by 16 hexadecimal digits. This is required for SCSI load or SCSI dump.

If the selected device type is **ECKD**, **NVMe** or **Tape**, this field is unavailable.

Logical unit number:

Specify the number of the logical unit as defined by FCP (according to the FCP/SCSI-3 specifications). This is the 64-bit binary number designating the unit number of the FCP I/O device, represented by 16 hexadecimal digits. This field is required for SCSI load or SCSI dump.

If the selected device type is **ECKD**, **NVMe**, or **Tape**, this field is unavailable.

Boot program selector:

This field identifies the program to load from the FCP-load device and contains a decimal value in the range from 0 to 30. This parameter provides the possibility of having up to 31 different boot configurations on a single disk device. This field should be set to 0 for optical media SCSI devices.

If the selected device type is **Tape** or **ECKD** and IPL type **CCW** is selected, this field is unavailable.

Boot record logical block address:

Specify the load block address if your file system supports dual-boot or booting from one of the multiple partitions. If no block address is specified, the logical-block address of the boot record is assumed to be zero. This feature could be used to IPL using a second or backup boot record, in case the original one is corrupted or overwritten by accident.

This field is unavailable if a device type of **ECKD** or **Tape** are selected.

Operating system load parameters:

Specify a variable number of characters to be used by the program that is loaded. This information will be given to the IPLed operating system and will be ignored by the machine loader. The IPLed operating system (or standalone dump program) has to support this feature. Any line breaks you enter are transformed into spaces before being saved.

If the selected device type is **Tape** or **ECKD** and IPL type **CCW** is selected, this field is unavailable.

Crypto

Use this window to customize information that controls how the logical partition activated by the profile uses the coprocessors and accelerators assigned to it. The settings are referred to here as *cryptographic controls*, and apply to the logical partition only if it is customized for using coprocessors and accelerators. This window allows you to:

- Add unassigned crypto(s) domain(s) to a logical partition for the first time.
- Edit assigned crypto(s) and domain(s) types to a logical partition already using cryptos and domains.
- Remove crypto(s) and domain(s) from a logical partition.

The assigned cryptographic domain index table displays the control domain and control and usage domain indexes which can be modified in the logical partition.

Control Domain

A logical partition's *control domains* are those cryptographic domains for which remote secure administration functions can be established and administered from this logical partition.

If you are using the Integrated Cryptographic Service Facility (ICSF), refer to ICSF documentation for information about ICSF basic operations.

If you are using a Trusted Key Entry (TKE) workstation to manage cryptographic keys, the TKE documentation provides information about selecting control domains and usage domains for a logical partition that is a TKE host or a TKE target.

Control and Usage Domain

A logical partition's *control and usage domains* are domains in the cryptos that can be used for cryptographic functions. The usage domains cannot be removed if they are online.

A logical partition's control domains can also include the usage domains of other logical partitions. Assigning multiple logical partitions' usage domains as control domains of a single logical partition allows using it to control their software setup.

If you are using the Integrated Cryptographic Service Facility (ICSF), refer to ICSF documentation for information about ICSF basic operations.

If you are using a Trusted Key Entry (TKE) workstation to manage cryptographic keys, the TKE documentation provides information about selecting control domains and usage domains for a logical partition that is a TKE host or a TKE target.

The assigned cryptos index table displays the cryptographic candidate list and cryptographic online list settings which can be modified in the logical partition.

Cryptographic Candidate List

The candidate list identifies which cryptos will be assigned to the logical partition. Cryptos cannot be removed if they are online.

Cryptographic Online List (from profile)
The online list identifies which cryptos will be brought online at the next activation. Changes to the online list do not affect the running system. You must activate the partition to bring the coprocessor or accelerators online.

You can work with the tables by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Edit
Allows you to "Edit Domains" on page 541 or "Edit Cryptos" on page 542 for the selected activation profile.

Remove
Allows you to remove selected control and usage domain settings or selected crypto candidate and online settings for the selected activation profile.

Add
Allows you to "Add Domains" on page 542 or "Add Cryptos" on page 542 for unassigned domains or unassigned crypto candidates for the selected activation profile.

The icons perform the following functions in the Assigned domains or crypto tables:

Select All
Selects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Deselect All
Deselects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header to change from ascending to descending order. Click **OK** when you have defined your preferred order.

Clear All Sorts
Returns the table back to the default order.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

You can find more detailed help on the following elements of this window:

Edit Domains

Use this window to change the domain type for the assigned domains in this activation profile.

Select the domain type you want to change for this activation profile.

Control
Identifies the control domain you want to change the cryptographic functions for the logical partition.

Control and usage
Identifies the control and usage domains that you want to change the cryptographic functions for the logical partition.

Additional functions on this window include:

OK
To perform the selected operation, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Domains

Use this window to select the unassigned domains and domain type to add to this activation profile. You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Select the domain type for this activation profile.

Control
Identifies the control domain that can use the cryptographic functions for the logical partition.

Control and usage
Identifies the control and usage domains that can use the cryptographic functions for the logical partition.

Additional functions on this window include:

OK
To add the selected unassigned domains to this activation profile, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Edit Cryptos

Use this window to change the crypto type for the assigned cryptos in this activation profile.

Select the crypto type you want to change for this activation profile.

Candidate
Identifies which cryptos will be assigned to the logical partition.

Candidate and online
Identifies which cryptos will be assigned and brought online at the next activations

Additional functions on this window include:

OK
To perform the selected operation, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Cryptos

Use this window to select the unassigned cryptos and crypto type to add for this activation profile. You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Select the crypto type for this activation profile.

Candidate
Identifies which cryptos will be assigned to the logical partition.

Candidate and online
Identifies which cryptos will be assigned and brought online at the next activations

Additional functions on this window include:

OK
To add the selected unassigned cryptos and crypto type for this activation profile, click **OK**.

Cancel

To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Time Offset

If the Central Processor Complex (CPC) uses an External Time Source such as an Server Time Protocol (STP) as its time source, and you chose to set the logical partition's clock using an offset from the External Time Source's time of day, use this window to set the offset and to choose how you want it applied when the logical partition's clock is set.

Note: The image profile includes this window only if the clock type selected on the **General** page of the logical partition's image profile is **Logical partition time offset**.

Offset
Specify or select the number of days, hours, and minutes you want to set for the offset from the External Time Source's time of day. You can set an offset within the following range:

- 0 to 999 days
- 0 to 23 hours
- 0, 15, 30, or 45 minutes

days
Specify or select the number of days, from 0 to 999, that you want to set for the offset from the External Time Source's time of day.

hours
Specify or select the number of hours, from 0 to 23, that you want to set for the offset from the External Time Source's time of day.

minutes
Specify or select the number of minutes, 0, 15, 30, or 45, that you want to set for the offset from the External Time Source's time of day.

Decrease system time value by the amount shown
To set the logical partition's clock *back* from the External Time Source's time of day by the number of days, hours, and minutes in the offset, select **Decrease system time value by the amount shown**. Use this setting to provide a local time zone WEST of GMT.

Increase system time value by the amount shown
To set the logical partition's clock *ahead* of the External Time Source's time of day by the number of days, hours, and minutes in the offset, select **Increase system time value by the amount shown**. Use this setting to provide a local time zone EAST of GMT or a date and time in the future.

Group page

This window displays a group profile name, group description, group capacity, and absolute capping value that can be customized in determining the allocation and management of processor resources assigned to the logical partition in the group.

In the processor type table, the absolute capping can be None or a number of processors value from 0.01 to 255.0. To change an absolute capping for a processor type in the group profile, select the current absolute capping setting in its field, then use the Customize Group Profiles window to specify the absolute capping for the selected processor type to indicate the new setting.

Group name
Use this entry field to enter a group name for logical partition(s) in the group.

Specify the group name that you want to work with:

- To customize a group name, enter a new name in the field.
- To view or customize an existing group name, select the arrow beside the field to list the names of existing group names. Then select a group name from the list to display its information.

Requirements for group names: A group name is required to save the information.

Group description
Use this entry field to specify a brief note, up to 50 characters long, that describes the contents or purpose of the profile.

Note: A description is recommended, but optional.

Group capacity
Use this entry field to specify a group capacity for all profiles belonging to this group.

Note: If you add a new logical partition member to the group, a new group capacity value does not take affect if other logical partition members of the group are active. All logical partition members of the group must be deactivated first before the new group capacity value can take affect. You can use the **Change LPAR Group Controls** task to change the group capacity value to the running system immediately.

Customize Group Profiles
Use this window to specify the absolute capping for the selected processor type assigned in the group profile.

None
To choose not to specify absolute capping, select **None**.

Number of processors (0.01 to 255.00)
To specify the number of processors, select **Number of processors (0.01 to 255.00)** and then in the input area specify a number in the range of 0.01 to 255.00 in increments of .01.

Additional functions on this window include:

OK
To save the new values and return to the previous window, click **OK**.

Cancel
To close the window without saving the changes you made and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Make a selection from the Profile Tree to view the group pages in the profile.

Customize Group Profiles

Use this window to specify the absolute capping for the selected processor type assigned in the group profile.

None
To choose not to specify absolute capping, select **None**.

Number of processors (0.01 to 255.00)
To specify the number of processors, select **Number of processors (0.01 to 255.00)** and then in the input area specify a number in the range of 0.01 to 255.00 in increments of .01.

Additional functions on this window include:

OK
To save the new values and return to the previous window, click **OK**.

Cancel
To close the window without saving the changes you made and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Deactivate

Accessing the Deactivate task for the CPC

Note: This task is not available when one or more managed systems have DPM enabled.

Deactivation is an orderly process for shutting down and turning off the system.

Shutting down and turning off the system, referred to also as *deactivating* the system, includes:

- Ending hardware and software activity.
- Clearing, releasing, and deallocating hardware resources.
- Turning off power.

You can use the Support Element workplace to start the task for deactivating the central processor complex (CPC). The target, or *object*, of a deactivation can be a CPC or an image. For more information about deactivating individual logical partitions, see "Accessing the Deactivate task for an object" on page 545.

Note: Although you can use the power switch on the CPC itself to turn it off, you should turn off CPC power by deactivating it instead. Unlike using the CPC's power switch, deactivating the CPC includes clearing, releasing, and deallocating its hardware resources before turning off its power.

To deactivate the CPC:

1. Open the **Deactivate** task.
2. Review the information on the Deactivate Task Confirmation window to verify the object you will deactivate is the CPC.
3. If the information is correct, click **Yes** to perform the deactivation.

   The Deactivate Progress window indicates the progress of the deactivation, and the outcome.
4. Click **OK** to close the window when the deactivation completes successfully.

   Otherwise, if the deactivation does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

After the CPC is deactivated, the CPC and the images are no longer operational.

Accessing the Deactivate task for an object

Note: This task is not available when one or more managed systems have DPM enabled.

You can use the Support Element workplace to start the task for deactivating an object of the central processor complex (CPC).

An *Image* is a set of CPC resources capable of running a control program or operating system. One or more images is created during a power-on reset of a CPC. Each logical partition is an image. You can use one or more images as deactivation targets to deactivate individual logical partitions.

To deactivate an object:

1. Open the **Deactivate** task.
2. Review the information on the Deactivate Task Confirmation window to verify the object you will deactivate.
3. If the information is correct, click **Yes** to perform the deactivation.

   The Deactivate Progress window indicates the progress of the deactivation, and the outcome.
4. Click **OK** to close the window when the deactivation completes successfully.

   Otherwise, if the deactivation does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

After the image is deactivated, the logical partition it supported is no longer operational. The CPC and images previously activated to support other logical partitions remain operational. Logoff the Support Element of each system that is to be powered off.

After logging off the integrated Support Element, shutdown the Hardware Management Console.

Define Clonable Internal Code Levels

Accessing the Define Clonable Internal Code Levels task

The **Define Clonable Internal Code Levels** task allows you to define internal code levels to save and send to the support system. The defined clonable internal code levels from a system are saved with an identifying name and password and sent to the support system, then later retrieved using the Hardware Management Console to bring another system to the identical internal code level. The Define Clonable Internal Code Levels window displays a list of all clonable internal code levels that have been defined. Click **Details...** to display the engineering change numbers and levels associated with a selected defined clonable internal code level. You can use the **Define Clonable Internal Code Levels** task to:

- Create a new defined clonable internal code level to be saved and sent to the support system.
- Replace an existing defined clonable internal code level with an updated level and send to the support system.
- Delete an existing defined clonable internal code level that is no longer needed.

Note: The Define Clonable Internal Code Levels window displays the machine serial number for the Support Element. You need this machine serial number when retrieving the clonable level definition data from the Hardware Management Console.

To define a clonable internal code level:

1. Open the **Define Clonable Internal Code Levels** task.

The Define Clonable Internal Code Levels window includes push buttons to perform tasks when working with defining a clonable internal code level. You can use the window to:

1. Type an identifying alphanumeric name and alphanumeric password of 1 to 8 characters in the **Name** and **Password** entry fields. Then, click **Create** to save a clonable internal code level to send to the support system.
2. Select a defined internal code level from the list to be replaced, then click Replace to replace the selected existing defined internal code level with an updated level to send to the support system.
3. Select a defined clonable internal code level from the list that is no longer needed, then click **Delete** to delete the existing defined clonable internal code level.

Make Internal Code Levels Clonable

Use the Make Internal Code Levels Clonable window to:

- Create a new defined clonable internal code level to be saved and sent to the support system.
- Replace an existing defined clonable internal code level with an updated level and send to the support system.
- Delete an existing defined clonable internal code level that is no longer needed.

The defined clonable internal code levels from a system are saved with an identifying name and password to the support system, and then later retrieved to bring another system to the identical internal code level. This window displays a list of all the current defined clonable internal code levels on the support element.

Defined clonable level list
Displays a possible list of defined clonable internal code levels for the system.

Details
To display the engineering change numbers and levels associated with the selected defined clonable internal code level, click **Details**.

Name
Type an identifying alphanumeric name to define and create a new clonable internal code level.

Password
Type an alphanumeric password of 1 to 12 characters.

Create
To create a new defined clonable internal code level, click **Create**.

Replace
To replace and update the current defined clonable internal code level, click **Replace**.

Delete
To delete the selected defined clonable internal code level, click **Delete**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Clonable Level Details

This Clonable Level Details window displays the engineering change numbers and levels associated with a selected defined clonable internal code level.

Clonable level details list
Displays a possible list of the engineering change numbers and levels associated with the defined clonable internal code level that was selected on the previous window.

OK
To close the window, click **OK**.

Help
To display help for the current window, click **Help**.

Delete LPAR Dump Data

Accessing the Delete LPAR Dump Data task

Dump data remains stored on the Support Element until it is either:

- Replaced by new dump data during an automatic dump.
- Deleted manually.

To manually delete dump data:

1. Open the **Delete LPAR Dump Data** task.
2. Use the window's controls to select the types of dump data you want to delete, then click **Delete** to delete them.

   Otherwise, if you only wanted to check the type, time, and date of previously dumped data, click **Cancel** to end the task *without* deleting the previously dumped data.

Delete Logical Partition Dump Data Confirmation

Use the **Delete LPAR Dump Data** task to delete the following types of service data:

Logical partition dump data
Logical partition control area information dumped while the central processor complex (CPC) is activated in logically partitioned (LPAR) mode.

Logical partition soft abend
Logical partition control area information automatically dumped by the hypervisor non-disruptively while the central processor complex (CPC) is activated in logically partitioned (LPAR) mode.

Coupling facility logical partition dump data
Coupling facility logical partition control area information dumped while a logical partition is activated in coupling facility mode.

Coupling facility diagnostics dump data
Coupling facility logical partition control area information dumped while a logical partition is activated in coupling facility mode. The non-disruptive dumps are generated by the Coupling Facility Control Code (CFCC). A maximum of 10 diagnostic dumps will be stored on the Support Element.

Firmware embedded framework dump data
CPC Firmware embedded framework control area information dumped while a logical partition is activated in IBM Secure Service Container (Secure Service Container) mode.

Ordinarily, you will not need to delete dump data manually.

Use this window to confirm or cancel your request to delete data from the Support Element hard disk.

Attention: Deleting dump data permanently removes it from the hard disk.

LPAR Data Dump List

If you intend to confirm your request to delete dump data, select one or more dumps to delete, then click **Delete**.

Dump Type
Indicates whether the dump data is from a logical partition .

Partition
If the dump data is from a coupling facility logical partition or CPC Firmware imbedded framework, this list displays the partition name.

Date
Displays the date the dump data was stored on the hard disk.

Time
Displays the time the dump data was stored on the hard disk.

The following additional functions are available from this window:

Delete
To confirm your request to delete the selected data dumps, click **Delete**.

Cancel
To cancel your request and close the window without deleting the dump data, click **Cancel**.

Help
To display help for the current window, click **Help**.

Disable Dynamic Partition Manager

Accessing the Disable Dynamic Partition Manager task

Use this task to disable Dynamic Partition Manager (DPM) mode on your system.

Note: This task is available only on the Support Element of a system that was ordered with the Dynamic Partition Manager (DPM) feature.

You can access this task from the main console page by selecting the Systems Management node or by selecting this task in the Tasks index. You can use either the SERVICE user ID or any user IDs that a system administrator has authorized to this task through customization controls in the **User Management** task.

To disable DPM mode on your system:

1. Select the system with Dynamic Partition Manager enabled.

2. Open the **Disable Dynamic Partition Manager** task. The Disable Dynamic Partition Manager window is displayed.
3. Click **Disable** to perform the operation.

   Note: The Support Element will restart to complete the operation.

Disable Dynamic Partition Manager

Use this window to disable Dynamic Partition Manager (DPM), remove all partitions, and unconfigure all adapters from the system.

Notes:

- The Support Element will restart to complete the operation.
- This task is available only when one or more managed systems have DPM enabled.

Additional functions on this window include:

Disable
To disable DPM for the CPC, click **Disable**.

Cancel
To close the window and confirm that DPM has not been disabled, click **Cancel**.

Help
To display help for the current window, click **Help**.

Display Adapter ID

Accessing the Display Adapter ID task

Use this task to display the adapter ID, location, and fanout type assigned to the InfiniBand channels.

To display the InfiniBand adapter ID:

1. Open the **Display Adapter ID** task.
2. The Display Assigned Adapter ID window lists the InfiniBand cage-card slot, location, fanout type and assigned adapter ID.
3. Click **OK** to exit the window.

Display or Alter

Accessing the Display or Alter task

A processor stores data in the following storage locations:

- Registers, which are special-purpose storage locations:
  - Program status word (PSW)
  - General purpose registers
  - Control registers
  - Floating point registers
  - Access registers
  - Prefix register
- Main storage locations:
  - Real storage
  - Real storage key
  - Primary virtual storage
  - Secondary virtual storage

  - Absolute storage
  - Home virtual storage
  - Virtual storage identified using access registers

Displaying or altering data in processor storage locations typically is done only by system programmers with experience in interpreting and altering the data. Follow your local procedures for determining when to display or alter data. You can use the Support Element workplace to display or alter the data in storage locations used by any eligible processor. Eligible processors include:

- Logical processors that support the images of logical partitions activated in operating modes other than coupling facility mode.

To display or alter data in processor storage:

1. Open the **Display or Alter** task.
2. Use the Display or Alter window controls to display or alter the data in the processor's storage locations.

Display or Alter

This window lists the storage locations used by the selected central processor (CP). Use this window to select the storage location for which you want to display or alter CP data.

- Registers
  - Current program status word (PSW)
  - General purpose registers
  - Control registers
  - Floating point registers
  - Floating point control register
  - Prefix register
  - Access registers
- Storage
  - Real storage
  - Real storage key
  - Primary virtual storage
  - Secondary virtual storage
  - Absolute storage
  - Home virtual storage
  - Virtual storage using access register 0-F
  - Virtual storage using access register 1-F

You can find more detailed help on the following elements of this window:

Apply

To display or alter a storage location you have chosen, click **Apply**.

Cancel

To close the window without choosing a storage location to display or alter, click **Cancel**.

Help

To display help for the current window, click **Help**.

Display or Alter registers

This window displays the data currently stored in the selected registers of the selected central processor (CP). The window title identifies the selected registers. Use the window's entry fields and controls to interpret and alter the register's data as needed.

Note: The purpose of the registers and the meanings of their possible values are beyond the scope of this online information. This window is intended for use by system programmers with experience in interpreting and altering the data in registers.

You can find more detailed help on the following elements of this window:

Register entry fields

The window provides two or four entry fields to use while displaying or altering the PSW. The number of entry fields depends on the addressing mode. When the window is displayed initially or refreshed, the fields display the current PSW. To alter the PSW, type the new PSW in the fields.

If there is more than one register, the entry field or fields for each register is labelled on the left by the hexadecimal number of the register.

The entry field or fields for each register display the hexadecimal value of the data currently stored in the register. Each field displays 4 bytes of data; each digit displays the hexadecimal value of 4 bits.

The data stored in the registers changes while the CP is operating, but the window displays the current data only at the time the window was displayed or refreshed. If the CP was operating at that time, or if you started the CP since then, the data displayed on the window very likely is not the data currently stored in the registers. You must stop the CP to display the current data. Click **Stop** to stop the CP. Upon stopping the CP, the window is refreshed to display the data currently stored in the registers.

To alter the data currently stored in the registers:

1. If the CP is operating, click **Stop** to stop it. Upon stopping the CP, the window is refreshed to display the data currently stored in the registers.
2. Type the hexadecimal value of new data in the entry fields for each register you want to alter.
3. To replace the current data with the new data, click **Save**. When you start the CP, it will resume operating with the new data.
4. To start the CP, click **Start**.

Selected CP

Displays the name of the selected CP and the current status of the CP (operating, stopped, looping) at the bottom left hand corner.

Addressing mode

Displays the storage addresses in 32-bit Enterprise System Architecture (ESA) or 64-bit Enterprise System Architecture Modal Extension (ESAME) mode. In ESA mode, the storage addresses are displayed as 4 bytes (32 bits). In ESAME mode, the storage addresses are displayed as 8 bytes (64 bits).

Instruction Address

Displays the hexadecimal address of the next instruction the CP will process when it resumes operating, when the CP is stopped. If the CP is operating, the address displayed in this field is not applicable.

Instruction Data

Displays the hexadecimal value of the instruction stored at the instruction address, when the CP is stopped. If the CP is operating, the address displayed in this field is not applicable.

Save

To replace the CP's current PSW with the PSW displayed in the entry fields, click **Save**.

Start

To start the CP, click **Start**.

Stop

To stop the CP, click **Stop**.

Refresh

To replace the PSW displayed in the entry fields with the CP's current PSW, click **Refresh**. This is available only if the PSW is read successfully.

Current program status word (PSW)

This window displays the current program status word (PSW) of the selected central processor (CP). Use the window's entry fields, display fields, and click buttons to interpret and alter the PSW as needed.

Note: The purpose of the PSW and the meanings of its possible values are beyond the scope of this online information. This window is intended for use by system programmers with experience in interpreting and altering the value of the PSW.

The CP's current PSW changes while the CP is operating, but the window displays the current PSW only at the time the window was displayed or refreshed. If the CP was operating at that time, or if you started the CP since then, the PSW displayed on the window very likely is not the CP's current PSW. You must stop the CP to display the CP's current PSW.

- The first field displays the hexadecimal value of bytes 0 through 3. The second field displays the hexadecimal value of bytes 4 through 7.
- If there are 4 entry fields, then the third field displays the hexadecimal value of bytes 8 through 11. The fourth field displays the hexadecimal value of bytes 12 through 15.
- Each digit displays the hexadecimal value of 4 bits.

To alter the current PSW:

1. If the CP is operating, click **Stop** to stop it. Upon stopping the CP, the window is refreshed to display the CP's current PSW.
2. Type the hexadecimal value for the new PSW.
3. To replace the current PSW with the new PSW, click **Save**. When you start the CP, it will resume operating with the new PSW.
4. To start the CP, click **Start**.

You can find more detailed help on the following elements of this window:

Display or Alter storage

This window displays the data currently stored in the selected type of storage for the selected central processor (CP). Use the window's entry fields, display fields, menu bar choices, and controls to interpret and alter the data in storage as needed.

Note: The purpose of the selected type of storage is beyond the scope of this online information. This window is intended for use by system programmers with experience in interpreting and altering the data in storage.

The window provides entry fields for you to use while displaying or altering data in the selected type of storage. When the window is displayed initially or refreshed, the fields display the data currently in storage. To alter the data in storage, type the new data in the fields. The window provides specific entry fields when the selected type of storage is real storage key. Otherwise, for types of storage *other than real storage key*, the following fields identify and display one page of data in storage.

You can find more detailed help on the following elements of this window:

Storage entry fields

The window provides fields for you to use while displaying or altering data in the selected type of storage. When the window is displayed initially or refreshed, the fields display the data currently in storage. To alter the data in storage, type the new data in the fields.

Selected CP

Displays the name of the selected CP and current status of CP (operating, stopped, looping) at the bottom left hand corner.

Addressing mode

Displays the storage addresses in 32-bit Enterprise System Architecture (ESA) or 64-bit Enterprise System Architecture Modal Extension (ESAME) mode. In ESA mode, the storage addresses are displayed as 4 bytes (32 bits). In ESAME mode, the storage addresses are displayed as 8 bytes (64 bits).

Instruction Address

Displays the hexadecimal address of the next instruction the CP will process when it resumes operating, when the CP is stopped. If the CP is operating, the address displayed in this field is not applicable.

Instruction Data

Displays the hexadecimal value of the instruction stored at the instruction address, when the CP is stopped. If the CP is operating, the address displayed in this field is not applicable.

Change range

To display the storage key for a particular 4KB range of real storage, type the storage address that begins the range in **Storage range**.

Save

To replace the current values of the storage key's bits with the values displayed in the entry fields, click **Save**. This is available only while the CP is stopped and if the values of the storage key's bits are read successfully.

Start

To start the CP, click **Start**.

Stop

To stop the CP, click **Stop**.

Refresh

To replace the storage displayed in the entry fields with the CP's current PSW, click **Refresh**.

Backward

To display the data stored in the previous page of storage locations, click **Backward**.

Forward

To display the data stored in the next page of storage locations, click **Forward**.

Real storage key

This window displays the storage key currently associated with a 4096 byte (4KB) range of real storage for the selected central processor (CP). Use the window's entry fields, display fields, menu bar choices, and controls to interpret and alter any storage key, as needed.

Note: The purpose of storage keys is beyond the scope of this online information. This window is intended for use by system programmers with experience in interpreting and altering storage keys.

The window provides storage address fields that identify the 4KB range of real storage associated with the storage key displayed on the window. You can use the fields, or **Backward** and **Forward** controls to display the storage key associated with a different 4KB range of real storage.

Storage range
Displays the addresses of the first byte and last byte in the 4KB range of real storage associated with the storage key displayed on the window. To display the storage key associated with a different 4KB range of real storage, you must change the address of only the first byte in the range. Type the new address in the entry field, then click **Change address**. The address must be a multiple of 4KB; that is, the last three digits in the address must be zeros.

Maximum address
Displays the address of the last byte of real storage.

When a storage key is displayed initially or refreshed, the fields display the current values of the storage key's bits. To alter the storage key, type new values in the fields.

Access control bits
Displays the hexadecimal value of bits 0-3 of the storage key. A storage key's access control bits are compared with the access key of the current program status word (PSW) when the CP attempts to access real storage in the storage key's 4KB range. If the PSW's access key matches the storage key's access control bits, the CP is permitted to store or refresh information in the storage key's 4KB range of real storage.

Fetch protection bit
Displays the binary value of bit 4 of the storage key. A storage key's fetch protection bit indicates the extent of key-controlled protection of real storage in the storage key's 4KB range. A bit value of 0 indicates key-controlled protection applies only to storing information, while a bit value of 1 indicates it applies to both storing and fetching information.

Reference bit
Displays the binary value of bit 5 of the storage key. The value of a storage key's reference bit is set to 1 whenever the CP stores or refreshes information in the storage key's 4KB range of real storage.

Change bit
Displays the binary value of bit 6 of the storage key. The value of a storage key's change bit is set to 1 whenever the CP stores information in the storage key's 4KB range of real storage.

Current bit values

The values of the storage key's bits change while the CP is operating, but the window displays the current values only at the time the storage key was displayed or refreshed. If the CP was operating at that time, or if you started the CP since then, the values displayed on the window likely are not the current values of the storage key's bits. You must stop the CP to display the current values.

To stop the CP, click **Stop**. Upon stopping the CP, the window is refreshed to display the current values of the storage key's bits.

Altering the bit values

To alter the current values of the storage key's bits:

1. If the CP is operating, click **Stop** to stop it. Upon stopping the CP, the window is refreshed to display the current values of the storage key's bits.
2. Type the new values in the entry fields of the bits you want to alter.
3. To replace the current values with the new values, click **Save**. When you start the CP, it will resume operating with the new values.
4. To start the CP, click **Start**.

You can find more detailed help on the following elements of this window:

Disruptive Task Confirmation

Disruptive Task Confirmation

This window is used to inform you that a disruptive task is about to be performed on a targeted object. The window displays the objects that are affected by the task, along with information about what happens to each of these objects.

Note: If necessary, you might be required to provide confirmation text input for each object and you might also be required to provide your password. These additional requirements ensure that you want to perform the disruptive task.

Affect object list

This list displays the set of objects that are affected by the disruptive task. It is possible for this list to contain more objects than those selected by you as targets for the task. If this is the case, it means that performing the task also affects these additional objects due to some relationship between the set of targets chosen by you and these additional objects.

It is important for you to review the affect this task has on all the listed targets to make sure the execution of the task has the expected results.

The following information is provided in the table:

System Name
Specifies the name of the object that is being disrupted by the task that is being executing.

Type
Specifies the type of the profile of the affected object.

OS Name
Specifies the associated operating system name of the affected object.

Note: You can have an object that is operating but does not have an operating system installed on it. In this case, the **OS Name** is blank. The **OS Name** can also be blank for non-LPAR virtual servers.

Status
Specifies the status of the affected object.

Confirmation Text
Describes the results of proceeding with the task for the affected object.

Confirmation text input

Provide the operating system name (preferred, if available) or the system name as input to the **Confirmation Text** fields. You can type the name in the field or copy the name from the table and paste it into the input area, then click **Confirm** to continue.

When you have provided the correct information, the affected object list indicates that your entries have been confirmed in the **Confirmation Status** column.

Note: If your user ID does not require additional confirmation text to perform the disruptive task then this input field is not available.

Password confirmation input

Use this input field to specify your user ID password which allows you to perform the disruptive task.

Note: If your user ID does not require a password to perform the disruptive task then this input field is not available.

Performing a disruptive task can have severe affects, therefore, you are required to confirm the execution of the task by specifying your user ID password in this input field. Once you provide the correct password, **Yes** is enabled and you can proceed with the disruptive task.

Yes

To continue with the execution of the disruptive task, click **Yes**.

No
To exit this window without continuing the execution of the disruptive task, click **No**.

Confirm
To continue with the execution of the disruptive task after providing confirmation text for each object, click **Confirm**.

Cancel
To exit this window without providing confirmation text or continuing the execution of the disruptive task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Domain Security

Accessing the Domain Security task

If you want to customize domain security, use this task to establish and maintain different domains for multiple Hardware Management Consoles and Support Element consoles attached to the same local area network (LAN). Ordinarily, to add or move a system from a domain is done from the Hardware Management Console, but this can be accomplished from the Support Element console.

The domain name and password of the console authorize its communication with the objects in its domain. They prevent unauthorized sources attached to the same local area network (LAN) from communication with other objects.

To define the domain security:

1. Open the **Domain Security** task. The Domain Security window is displayed.
2. Specify a domain name and domain password. Select the option with which you want the domain to apply.
3. Click **OK** to proceed with the change.

Domain Security

Use this window to change the name or password of the domain of this Support Element console.

The “Current domain name” on page 557 is displayed on the window. If **MANUFACTURING DEFAULT** is displayed, it indicates that default domain security is in effect for this console.

The “Current password status” on page 557 indicator is displayed on the window. The password itself is not displayed. If **SET** is displayed, it indicates that the password has been set for this console. If **NOT SET** is displayed, it indicates that the password has not been set for this console.

Important: See Important domain security information about using this task correctly.

Default domain security is the type of domain security that is initially set for new Support Element consoles and for new, undefined objects.

The intent of default domain security is to allow connecting Hardware Management Consoles to initially communicate with the Support Element in a secure manner. This default domain name and password is changed to match that of the Hardware Management Console that first defines this Support Element.

Customized domain security is a type of domain security you can set for a Hardware Management Console and its defined Support Element consoles. The intent of customized domain security is the same as that of default domain security, but with an extra level of security.

Like default domain security, it allows connecting a Hardware Management Console and Support Element consoles to a Local Area Network (LAN) that might attach other systems and devices. It also provides secure communications between the console and its objects that prevents other systems and devices on the same LAN from being used to control the objects. Unlike default domain security, it provides secure communications between the console and its defined objects that prevents other Hardware Management Consoles on the same LAN from being used to control its objects.

Customized domain security can provide complete domain security within a parallel sysplex while one or more Hardware Management Consoles are attached to the same LAN as alternate consoles for the sysplex and while one or more Hardware Management Consoles are attached to the same LAN as primary and alternate consoles for other sysplexes.

Current domain name

Displays the name that is currently assigned to the domain of the console.

This current domain name displays one of the following:

MANUFACTURING DEFAULT
Indicates that default domain security currently is in effect for the console.

Any other *name*
Indicates that customized domain security currently is in effect for the console. The current name of the domain is *name*.

Domain Name

Use this field to specify a new name for the domain of this Support Element console.

The domain of a Support Element console defines the set of Hardware Management Consoles that can manage the Support Element

The domain name and password of the console authorize its communication with the objects in its domain. They prevent unauthorized sources that are attached to the same LAN from communicating with the objects.

Requirements for a domain name
A new domain name is optional. But to change domain security, you must change either the domain name or password, or both. To keep the current domain name and change only the domain password, leave this field blank.

A domain name can be from 1 to 8 characters long. It cannot have special characters or embedded blanks. Valid characters for a domain name are numbers **0** through **9** and alphabetic letters **A** through **Z**.

Note: Domain names are not case-sensitive. All alphabetic characters are saved in uppercase.

Current password status

Indicates whether the password is set for the domain of the console. The password itself is not displayed.

This current password status displays one of the following:

SET
Indicates that the password has been set for the domain of the console.

NOT SET
Indicates that the password has not been set for the domain of the console.

New password

Use this field to specify the new password to the domain of this console.

Note: The password is not displayed as you specify it; asterisks display instead.

The domain name and password of the console authorize its communication with the objects in its domain. They prevent unauthorized sources that are attached to the same LAN from communicating with the objects.

Requirements for a domain password of eight or fewer characters

A new domain password is optional. But to change domain security, you must change either the domain name or password, or both. To keep the current domain password and change only the domain name, leave this field blank.

A password can be 6 - 8 characters long. It cannot have special characters or embedded blanks. Valid characters for a password are numbers **0** through **9** and alphabetic letters **A** through **Z**.

Note: Passwords are not case-sensitive. All alphabetic characters are saved in uppercase.

The first and last character of a password must be a letter.

A password must include at least one number, but it cannot be the first or last character in the password.

A password cannot include a sequence of 3 characters that are the same.

Requirements for a domain password of nine or more characters

A domain that uses this longer password format cannot include Version 2.13.1 and prior HMC consoles or defined objects.

A new domain password is optional. But to change domain security, you must change either the domain name or password, or both. To keep the current domain password and change only the domain name, leave this field blank.

A password can be from nine to 64 characters long. It can have special characters that include:

` ~ ! @ # $ % ^ & * ( ) - _ = + [ ] { } \ | ; : ' " , . < > / ?

It cannot have embedded blanks. In addition to the special characters listed, valid characters for a password are numbers **0** through **9** and uppercase and lowercase alphabetic letters **A** through **Z**.

Note: Passwords are case-sensitive.

Verify password

Use this field to specify again the same password you specified in the **New password** field.

Note: The password is not displayed as you specify it; asterisks display instead.

Important: You do not need to write down or remember the domain password. After it is applied, it is used only for internal communication between this console and the objects in its domain. You are required to know the password to perform any other tasks at this console. If you need to assign the same password to other consoles you want in the same domain, it is recommended you do so promptly.

Change console domain name and/or password

To assign the domain name, password, or both to this console only, select **Change console domain name and/or password**.

Note: Changing the name and password for the domain of only this console affects the ability for Hardware Management Consoles to communicate with this console.

Reset to manufacturing default domain name and password

The manufacturing default domain is the type of domain security that is initially set for new consoles and for new, undefined objects. To reset the domain name and password to the default domain name and password, select **Reset to manufacturing default domain name and password**.

Note: This option appears if you are using the SERVICE default user ID or a user ID that is assigned Service Representative roles.

Additional options on this window are available:

OK
To assign the new domain name and password to the Support Element you want to include in the new domain or to reset the domain name and password to the default, click **OK**.

Cancel
To close the window without changing the current settings for domain security, click **Cancel**.

Help
To display help for the current window, click **Help**.

Important domain security information

Consequences of customizing domain security

- Changing the domain of a support element console will remove it from its current domain, regardless of what other consoles are still in that domain. This may strand the Support Element console outside the domain of any Hardware Management Console, effectively isolating it.
- Applying a customized domain name or password to consoles or defined objects currently in the default domain removes them from the default domain. Afterwards, you must contact the support system for assistance if you want to move consoles or objects from a customized domain back into the default domain.
- If you are changing the domain security settings on the primary Support Element and it is communicating with the alternate Support Element, performing a mirror prior to restarting the primary Support Element will put the domain security settings into effect on the alternate SE after the next alternate Support Element restart.
- The domain security settings should only be changed on the alternate Support Element if it is not communicating with the primary Support Element.

When to use this task

Use this task only when you want customized domain security. Customize domains to establish and maintain different domains for **multiple** Hardware Management Consoles and Support Elements attached to the same LAN.

Dump LPAR Data

Accessing the Dump LPAR Data task

Most service data is collected and stored automatically by the Support Element of the central processor complex (CPC). This includes logical partition dump data, coupling facility logical partition dump data, and CPC Firmware embedded framework dump data.

Logical partition dump data is control area information that is automatically collected and stored if logical partition errors are detected. Collecting and storing information is often referred to as *dumping data*.

Coupling facility logical partition dump data is control area information that is automatically collected and stored if coupling facility logical partition errors are detected while a logical partition is operating in coupling facility mode.

CPC Firmware embedded framework dump data is control area information that is automatically collected and stored if CPC Firmware embedded framework errors are detected while a logical partition is operating in IBM Secure Service Container (Secure Service Container) mode.

Like other types of service data, logical partition dump data , coupling facility logical partition dump data, and CPC firmware embedded framework dump data assist in servicing the CPC. Sending dump data to your support system is necessary only when dump data is requested.

If the dump data requested is not available, or if it is available but was not dumped recently, you can manually dump the data first, then send it and any other requested service data to your support system.

Note: If you are not certain whether dump data is already stored on the Support Element, or whether it was dumped recently, you can use the **Delete LPAR Dump Data** task to check. Starting the task displays a window that lists the types of dump data, if any, already stored on the Support Element, and displays the time and date the data was dumped. See the **Delete LPAR Dump Data** task for instructions for starting the task. After you've checked the type, time, and date of previously dumped data, you will be able to cancel the task *without* deleting the previously dumped data.

To manually dump data:

1. To dump logical partition data, the CPC must be power-on reset.
2. To dump logical partition dump data, locate the CPC:
   a. Locate the **CPC** to work with.
3. To dump coupling facility logical partition dump data, the CPC must be power-on reset, and a logical partition must be activated in coupling facility mode.
   a. Locate the coupling facility **Image** you want to work with.
4. To dump CPC Firmware embedded framework data:
   a. Locate the Secure Service Container **Image** you want to work with.
5. Open the **Dump LPAR Data** task.

   This opens the dump window for the target object.

   Note: If a message notifies you that dump data is already stored on the Support Element, you must delete it before you can manually perform another dump. For more information and instructions, see the **Delete LPAR Dump Data** task.
6. Use the window's controls to select the type of dump you want to perform, then click **OK** to start the dump.

Dump Coupling Facility Logical Partition Data

Use this window to use the dump utility manually to perform a dump for the selected coupling facility logical partition.

While a logical partition is operating in coupling facility mode, the dump utility automatically collects and stores control area information if coupling facility errors are detected. But you can also use this window whenever necessary to collect and store the control area information manually. In either case, the control area information is stored on the support element hard disk.

Type of dump
Select the type of dump you want to perform, then click **OK**.

Coupling facility partition control area information (Disruptive)
To perform a disruptive dump, click **Coupling facility partition control area information (Disruptive)**.

Note: Use this task only as directed by your support system.

This procedure is disruptive and will:

- Cancel all operations currently in progress in the coupling facility logical partition.
- Stop logical processors before coupling facility logical partition information is dumped to the hard disk. The processors remain stopped after the dump completes.
- Delete any data in the coupling facility that belongs to other images using the coupling facility. This will disrupt control program operations of those images.

Note: It is recommended you allow the operations to complete, or stop the operations, and stop the images from using the coupling facility, before performing the dump.

Coupling facility partition control area information (Not disruptive)
To perform a non-disruptive dump, click **Coupling facility partition control area information (Not disruptive)**.

Note: Use this task only as directed by your support system.

This procedure is not disruptive to the operations of the selected coupling facility logical partition.

However, it will temporarily prevent the coupling facility from responding to requests from control programs of other images using the coupling facility. This will disrupt control program operations of those images.

Note: It is recommended you allow the operations to complete, or stop the operations, and stop the images from using the coupling facility, before performing the dump.

OK
To perform the selected type of dump, click **OK**.

Cancel
To close the window without performing a dump, click **Cancel**.

Help
To display help for the current window, click **Help**.

Confirm the Action

Use this window to confirm or cancel your request to perform a disruptive dump for the selected coupling facility logical partition.

Attention: Confirming a request to perform a disruptive dump:

- Cancels all operations currently in progress in the coupling facility logical partition.
- Stops logical processors before coupling facility logical partition control area information is dumped to the hard disk. The processors remain stopped after the dump completes.
- Deletes any data in the coupling facility that belongs to other images using the coupling facility. This will disrupt control program operations of those images.

Note: It is recommended you allow the operations to complete, or stop the operations, and stop the images from using the coupling facility, before performing the dump.

Attention: Confirming a request to perform either a disruptive or non-disruptive dump requires deleting at least one of the two coupling facility data dumps already stored on the support element hard disk.

Dump list
Displays the name of the coupling facility logical partition the dump data is from, the date the dump data was stored on the hard disk, and the time the dump data was stored on the hard disk.

Select one or more current dumps to delete, then click **Dump**.

Dump
To confirm your request to perform the disruptive dump, and to delete the selected current dumps, click **Dump**.

Cancel
To cancel your request and close the window without performing a new dump or deleting any current dumps, click **Cancel**.

Help
To display help for the current window, click **Help**.

Dump Logical Partition Data

Use this window to use the dump utility manually to perform a dump for the Central Processor Complex (CPC).

While the CPC is operating in Logically Partitioned (LPAR) Mode, the dump utility automatically collects and stores control area information if logical partition errors are detected. But you can also use this window whenever necessary to collect and store the control area information manually. In either case, the control area information is stored on the Support Element hard disk.

Type of dump
Select the type of dump you want to perform, then click **OK**.

Logical partition control area information (Disruptive)
To perform a disruptive dump, click **Logical partition control area information (Disruptive)**.

Note: Use this task only as directed by support system.

This procedure is disruptive. It will cancel all operations in progress on the CPC's logical partitions. Physical processors are stopped before logical partition control area information is dumped to the hard disk. The processors remain stopped after the dump completes.

Logical partition control area information (Not disruptive)
To perform a non-disruptive dump, click **Logical partition control area information (Not disruptive)**.

Note: Use this task only as directed by your support system.

This procedure is not disruptive. It will not affect any operations in progress on the CPC's logical partitions.

OK
To perform the selected type of dump, click **OK**.

Cancel
To close the window without performing a dump, click **Cancel**.

Help
To display help for the current window, click **Help**.

Confirm the Action

Use this window to confirm or cancel your request to perform a dump for the central processor complex (CPC).

Attention: Confirming a request to perform a disruptive dump:

- Disrupts the operation of all the CPC's logical partitions.
- Stops all physical processors before logical partition control area information is dumped to the hard disk. The processors remain stopped after the dump completes.

Attention: Confirming a request to perform either a disruptive or non-disruptive dump requires deleting the logical partition dump data already stored on the Support Element hard disk.

Dump
To confirm your request to perform the new dump and delete the current dump, click **Dump**.

Cancel
To cancel your request and close the window without performing a new dump or deleting the current dump, click **Cancel**.

Help
To display help for the current window, click **Help**.

Dump CPC Firmware embedded framework data

Use this window to use the dump utility manually to perform a selected CPC Firmware embedded framework dump data.

While a logical partition is operating in a Secure Service Container mode, the dump utility automatically collects and stores control area information if CPC Firmware embedded framework errors are detected. But you can also use this window whenever necessary to collect and store the control area information manually. In either case, the control area information is stored on the Support Element hard disk.

Type of dump
Select the type of dump you want to perform, then click **OK**.

CPC Firmware embedded framework dump data (Disruptive)
To perform a disruptive dump, click **CPC Firmware embedded framework dump data (Disruptive)**.

Note: Use this task only as directed by your support system.

This procedure is disruptive and will:

- Cancel all operations currently in progress in the CPC Firmware embedded framework.
- Stop logical processors before CPC Firmware embedded framework information is dumped to the hard disk. After the dump completes, a reload and a restart of the CPC Firmware embedded framework will occur.
- Delete any data in the CPC Firmware embedded framework that belongs to other images using the CPC Firmware embedded framework. This will disrupt control program operations of those images.

Note: It is recommended you allow the operations to complete, or stop the operations, and stop the images from using the CPC Firmware embedded framework, before performing the dump.

CPC Firmware embedded framework dump data (Not disruptive)
To perform a non-disruptive dump, click **CPC Firmware embedded framework dump data (Not disruptive)**.

Note: Use this task only as directed by your support system.

This procedure is not disruptive to the operations for the selected CPC Firmware embedded framework.

However, it will temporarily prevent the CPC Firmware embedded framework from responding to requests from control programs of other images.

Note: It is recommended you allow the operations to complete, or stop the operations, and stop the images from using the CPC Firmware embedded framework dump data, before performing the dump.

OK
To perform the selected type of dump, click **OK**.

Cancel
To close the window without performing a dump, click **Cancel**.

Help
To display help for the current window, click **Help**.

Dump Machine Loader Data

Accessing the Dump Machine Loader Data task

Most service data is collected and stored automatically by the Support Element of the central processor complex (CPC). This includes logical partition dump data and coupling facility logical partition dump data.

Logical partition dump data is control area information that is automatically collected and stored if logical partition errors are detected. Collecting and storing information is often referred to as *dumping data*.

Coupling facility logical partition dump data is control area information that is automatically collected and stored if coupling facility logical partition errors are detected while a logical partition is operating in coupling facility mode.

Like other types of service data, logical partition dump data and coupling facility logical partition dump assist the support system in servicing the CPC. Like other types of service data, sending dump data to the support system is necessary only when dump data is requested by the support system.

If the dump data requested by the support system is not available, or if it is available but was not dumped recently, you can manually dump the data first, then send it and any other requested service data to the support system.

Note: If you are not certain whether dump data is already stored on the Support Element, or whether it was dumped recently, you can use the **Delete LPAR Dump Data** task to check. Starting the task displays a window that lists the types of dump data, if any, already stored on the Support Element, and displays the time and date the data was dumped. After you've checked the type, time, and date of previously dumped data, you will be able to cancel the task *without* deleting the previously dumped data.

To manually dump data in LPAR or coupling facility mode:

1. Open the **Dump LPAR Data** task.

   This opens the dump window for the target object.

   Note: If a message notifies you that dump data is already stored on the Support Element, you must delete it before you can manually perform another dump. For more information and instructions, see the **Delete LPAR Dump Data** task.
2. Use the window's controls to select the type of dump you want to perform, then click **OK** to start the dump.

Edit Frame Layout

Accessing the Edit Frame Layout task

This task provides a graphic view of the physical location of the hardware objects that are defined to this Hardware Management Console. Each object is shown with its frame designation and position within the frame. By opening (double-clicking on) the object, additional information is provided:

- Machine type
- Model
- Serial number
- Device location

This task also shows the locations in the frames that are available for adding or moving a device. In addition to adding or moving devices, the service representative can also remove devices or add frames.

To add, remove, or move hardware objects that are defined to the Hardware Management Console:

1. Open the **Edit Frame Layout** task. The Edit Frame Layout window is displayed.

   Note: If you select more than one object, the Object Selection window is displayed prompting you to select a single CPC on which to perform the task.
2. Click **Save** when you have completed the task and want to save your changes.

Edit Frame Layout

This window displays graphically the current hardware configuration information for a machine.

Use this window after changing the actual hardware configuration of a machine to update its hardware configuration information.

Changing configuration information

Use the menus from the window to change the hardware configuration information for the frame, device, or open area you changed in the actual hardware configuration.

For step-by-step instructions about changing configuration information, select the change you made to the actual hardware configuration from the following:

- Installed a new device
- Installed a new frame
- Moved a device
- Removed a device

- Removed a frame

Frame and device graphics

Frame and device graphics indicate the layout of frames, and the location and size of devices, as described by the current hardware configuration information for the machine.

Use the mouse to select graphics and to display the menus of actions you can use on the selected graphic.

Frame
Represents an actual frame and its location in the machine.

Using the left mouse button, click any open area in the frame to display a menu of frame actions.

Device
Represents an actual device, and its size and location in a frame.

Using the left mouse button, click on a device to display a menu of device actions.

Using the left mouse button, double-click on a device to display the current, detailed hardware configuration information for the device.

Open area
Represents the size and location of empty space in a frame.

Using the left mouse button, click on an empty space to display a menu of frame actions.

Additional functions on this window include:

Machine Type
Displays the machine type of the machine.

Machine Model
Displays the model number of the machine.

Serial Number
Displays the serial number of the machine.

Save and Exit
To save the hardware configuration information represented by the frame layout currently displayed, to close the window, and to end this task, click **Save and Exit**.

Hardware configuration information for each Central Processor Complex (CPC) is stored on its Support Element.

Hardware configuration information for each device is stored on the support element of the CPC associated with the device.

Add Frame...
To add a frame to the hardware configuration, click **Add Frame...**.

Cancel
To close the window without saving changes you made to the frame layout, click **Cancel**.

Help
To display help for the current window, click **Help**.

Installed a new device

Follow this procedure to add information about a new device you installed.

On the **Edit Frame Layout** window:

1. Using the left mouse button, click on the open area of the frame where you installed the device.

   The selected open area flashes, and the frame actions menu is displayed.
2. Verify whether the flashing open area includes the location where you installed the new device, then:

   a. If the flashing open area includes the new device location, continue to the next step.

b. Otherwise, select **Deselect open area**, then start again with step 1.

3. Select **Add device** from the menu.

   The first of two **Add device** windows is displayed.

4. Use the windows to provide information about the exact location of the device you added, and its specific product information.

   Request help for the windows for additional information about using them to complete this step and to add the device to the frame layout.

   The **Edit Frame Layout** window is displayed again. The updated frame layout is displayed the device you added to the selected open area.

5. Click **Save and Exit** on the **Edit Frame Layout** window to save the new device information with the hardware configuration information for the machine.

Installed a new frame

Follow this procedure to add information about a new frame you installed.

On the **Edit Frame Layout** window:

1. Click **Add Frame...**.

   The **Add Frame** window is displayed.

2. Use the window to specify the frame label.

   Request help for the window for additional information about using it to complete this step and to add the frame to the frame layout.

   The **Edit Frame Layout** window is displayed again. The updated frame layout displays the frame you added to the machine.

3. Select **Save and Exit** on the **Edit Frame Layout** window to save the new frame information with the hardware configuration information for the machine.

Moved a device

Follow this procedure to change information about the location of a device you moved.

On the **Edit Frame Layout** window:

1. Using the left mouse button, click on the device you moved.

   The selected device flashes, and the device actions menu is displayed.

2. Select **Move device** from the menu.

   The first of two **Move device** windows is displayed.

3. Use the windows to specify which frame you moved the device to, and the exact location of the device in that frame.

   Request help for the windows for additional information about using them to complete this step and to move the device within the frame layout.

   The **Edit Frame Layout** window is displayed again. The updated frame layout displays the device in its new location.

4. Select **Save and Exit** on the **Edit Frame Layout** window to save the new device location with the hardware configuration information for the machine.

Removed a device

Follow this procedure to delete information about a device you removed.

On the **Edit Frame Layout** window:

1. Using the left mouse button, click on the device you removed.

The selected device flashes, and the device actions menu is displayed.

2. Select **Delete device** from the menu.

   A message is displayed to identify the device you selected to delete.

3. Use the message to confirm your request to delete the selected device.

   The **Edit Frame Layout** window is displayed again. The updated frame layout no longer is displayed the device you removed.

4. Select **Save and Exit** on the **Edit Frame Layout** window to delete the device information from the hardware configuration information for the machine.

Removed a frame

Follow this procedure to delete information about a frame you removed.

On the **Edit Frame Layout** window:

1. A frame must be empty before you can delete it. Delete all devices in the frame.

   Note: Delete a device after you removed the device from the actual frame.

2. Using the left mouse button, click on the open area of the empty frame you removed.

   The selected open area flashes, and the frame actions menu is displayed.

3. Select **Delete empty frame** from the menu.

   A message is displayed to identify the frame you selected to delete.

4. Use the message to confirm your request to delete the selected frame.

   The **Edit Frame Layout** window is displayed again. The updated frame layout no longer displays the frame you removed.

5. Select **Save and Exit** on the **Edit Frame Layout** window to delete the frame information from the hardware configuration information for the machine.

Device actions

Use this menu to select an action for working with the selected device.

A device flashes to indicate it is currently selected.

Menu choices

Move device
To change the location of the selected device, select this menu choice.

Change the location of a device in the frame layout only after you moved the device within the actual machine.

Delete device
To delete the selected device from the frame layout, select this menu choice.

Delete a device from the frame layout only after you removed the device from the actual frame.

Device details
To display the current, detailed hardware configuration information for the selected device, select this menu choice.

Note: Double-click the left mouse button on a device for another way to display its hardware configuration information.

Deselect device
To close the device actions menu and deselect the selected device, select this menu choice.

Add Fibre Trunk
To add a Fibre Trunk to the machine, select this menu choice.

Update Fibre Trunk
To change the location or serial number of a Fibre Trunk, or to view the Fibre Trunks in the system, select this menu choice.

Delete Fibre Trunk
To delete a Fibre Trunk and deselect the selected device, select this menu choice.

Frame actions

Use this menu to select an action for working with either:

- The selected empty frame
- The selected open area in a frame

An open area flashes to indicate it is currently selected.

Menu choices

Add device
To add a device to the selected open area of a frame, select this menu choice.

Add a device to the frame layout only after you installed a new device in the actual frame.

Delete empty frame
To delete a frame from the frame layout, select this menu choice.

Note: This choice is available only when the frame is empty.

Delete a frame from the frame layout only after you removed the frame from the actual machine.

Deselect open area
To close the frame actions menu and deselect the selected open area, select this menu choice.

Add Fibre Trunk
To add a Fibre Trunk to the machine, select this menu choice.

Update Fibre Trunk
To change the location or serial number of a Fibre Trunk, or to view the Fibre Trunks in the system, select this menu choice.

Delete Fibre Trunk
To delete a Fibre Trunk and deselect the selected device, select this menu choice.

Device actions

Use this menu to select an action for working with the selected device.

A device flashes to indicate it is currently selected.

Menu choices

Move device
To change the location of the selected device, select this menu choice.

Change the location of a device in the frame layout only after you moved the device within the actual machine.

Delete device
To delete the selected device from the frame layout, select this menu choice.

Delete a device from the frame layout only after you removed the device from the actual frame.

Device details
To display the current, detailed hardware configuration information for the selected device, select this menu choice.

Note: Double-click the left mouse button on a device for another way to display its hardware configuration information.

Deselect device
To close the device actions menu and deselect the selected device, select this menu choice.

Add Fibre Trunk
To add a Fibre Trunk to the machine, select this menu choice.

Update Fibre Trunk
To change the location or serial number of a Fibre Trunk, or to view the Fibre Trunks in the system, select this menu choice.

Delete Fibre Trunk
To delete a Fibre Trunk and deselect the selected device, select this menu choice.

Add Frame

Use this window to specify the label and the type of the frame added to the hardware configuration of the machine you are working with.

Select the frame label and frame type from those displayed, and enter the serial number of the frame, then click **Add Frame**.

Frame label
To choose the label of the frame added to the hardware configuration of the machine, use the down arrow to select a **Frame label**.

Frame Types
Select a frame type from the list provided.

Serial number

Specify the serial number assigned to the frame.

Add Frame
To add the specified frame to the frame layout of the machine, click **Add Frame**.

Add a frame to the frame layout only after you installed a new frame in the actual machine.

Note: Click **Save and Exit** on the **Edit Frame Layout** window to save the frame information with the hardware configuration information for the machine.

Cancel
To close the window and not add a frame, click **Cancel**.

Help
To display help for the current window, click **Help**.

Frame Details

Use this window to verify the detailed hardware configuration information for a selected frame. This window also provides the ability to change the detailed hardware configuration information.

Frame label
Displays the name or identity of the frame.

Description
Displays the description of the frame.

Serial number
Displays the serial number of the frame.

Change Frame Details...
To change the frame details from the information that is displayed, click **Change Frame Details...**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Change Frame Details

Use this window to verify or change the detailed hardware configuration information for a selected frame.

Frame label
Displays the name or identity of the frame.

Description
Displays the current description of the frame.

Description (new)
Specify the new description of the frame.

Serial number
Displays the current serial number of the frame.

Serial number (new)
Specify the new serial number of the frame.

Save
To change the frame details to the information you entered, click **Save**.

Cancel
To close the window without changing the frame details, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Cage

Use this window to define a cage in your hardware configuration layout. Select a cage from the table, then click **Add Cage**.

Cage table
Use this window to define a cage in your configuration layout. This table lists the available cages by description and device UPC card serial number.

Select one, then click **Add Cage...** to define that cage in your configuration layout.

Add Cage...
To define the selected cage in your hardware configuration, click **Add Cage...**.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Cage

Use this window to add a cage to the hardware configuration. Select the location of the cage, then click **Add Cage**.

Cage Addresses
This table displays the addresses of the cages available to add to the hardware configuration. Select a cage to add to the hardware configuration and specify the serial number of the device, then click **Add Cage**.

Serial number
Specify the serial number of the device.

Add Cage
To add the selected cage to the hardware configuration, click **Add Cage**.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Device

Use this window to select the device added to the hardware configuration of the machine you are working with.

Select the device you added, then click **Add Device...**.

Device table
This table displays a list of devices that were recently added to your hardware configuration by description, device serial number, and associated CPC name and location.

Select a device, then click **Add Device...**.

Add Device...
To add the selected device to the fame layout of the machine, click **Add Device...**.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Device

Use this window to select the device added to the hardware configuration of the machine you are working with.

Select from the list the device you added, then click **Add Device...**. Another window is displayed for you to provide specific hardware configuration information about the device.

Machine type
Displays the machine type of the machine you added a device to.

Machine model
Displays the model number of the machine you added a device to.

Devices
Displays the name, or type, and description of devices that can be added to the machine.

Add Device...
To add the selected device to the frame layout of the machine, click **Add Device...**.

Cancel
To close the window and not add the device to the frame layout, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Device

Use this window to provide product and location information about a device added to the hardware configuration.

Device
Displays the name, or type, and description of the device added to the machine.

Serial number
Specify the serial number of the device.

Frame
Displays the label of the frame you added the device to.

Exact location
Select the location of the device. Device locations are identified by four characters.

The first character of a device location identifies the frame label.

The next two characters identify the vertical location of the device, relative to the bottom of the frame. Vertical locations are identified by two digits, decimal numbers from bottom to top, beginning with the number 01.

The last character identifies the horizontal location of the device, relative to the left side of the front of the frame. Horizontal locations are identified by letters from left to right, beginning with the letter A.

Associated CPC
Select the Central Processor Complex (CPC) that the device is physically connected to.

The CPC you select becomes associated with the device. The hardware configuration information for a machine is stored on the support elements of its CPCs. A support element stores information only for its CPC and the devices associated with the CPC.

Associating a device with a CPC is necessary to identify the support element used for storing the device information, and to indicate the device is physically connected to the CPC. But associating a device with a CPC does not affect which CPCs can be configured to use the device.

Add Device
To add the device to the frame layout for the machine, click **Add Device**.

Note: Click **Save and Exit** on the **Edit Frame Layout** window to save the device information with the hardware configuration information for the machine.

Cancel
To close the window and not add the device to the frame layout, click **Cancel**.

Help
To display help for the current window, click **Help**.

Device Details

Use this window to view device details. Detailed hardware configuration information for a selected device is displayed.

To change the device details, specify the device serial number and select the associated CPC, then click **Change Device Details**.

Device
Displays the name or type of the device.

Description
Displays a brief description of the device.

Location
Identifies the location of the device.

Serial number
Displays the serial number of the device. You can also specify another serial number.

Associated CPC
Displays the name and location of the Central Processor Complex (CPC) that the device is physically connected to.

The CPC you select becomes associated with the device. The hardware configuration information for a machine is stored on the support elements of its CPCs. A support element stores information only for its CPC and the devices associated with the CPC.

Associating a device with a CPC is necessary to identify the support element used for storing the device information, and to indicate the device is physically connected to the CPC. But associating a device with a CPC does not affect which CPCs can be configured to use the device.

Associated devices

This table displays the name and location of devices associated with the Central Processor Complex (CPC).

Change Device Details
To change the device details to the device information currently displayed, click **Change device details**.

Note: Click **Save and Exit** on the **Edit Frame Layout** window to save the updated device information with the hardware configuration information for the machine.

Hardware configuration information for each Central Processor Complex (CPC) is stored on its support element.

Hardware configuration information for each device is stored on the support element of the CPC associated with the device.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Move Device

Use this window to specify a label of the frame where you installed a device removed from another location in the machine.

Use the drop downs choices to select the frame information, then select **Move Device**.

Device
Displays the name or type of the device you moved.

Description
Displays a brief description of the device you moved.

Previous location
Displays the location of the device currently stored in the hardware configuration information.

Frame
From the drop down choices, select the label of the frame where you reinstalled the device you moved.

Exact location
Select the location in the frame, in the lower, left-hand corner, where you reinstalled the device you moved.

Device locations are identified by four characters.

The first character of a device location identifies the frame label.

The next two characters identify the vertical location of the device, relative to the bottom of the frame. Vertical locations are identified by two digits, decimal numbers from bottom to top, beginning with the number 01.

The last character identifies the horizontal location of the device, relative to the left side of the front of the frame. Horizontal locations are identified by letters from left to right, beginning with the letter A.

Move device
To delete the device from its current frame in the frame layout, and to add it to its new frame, select **Move device**.

Note: Click **Save and Exit** on the **Edit Frame Layout** window to save the updated device information with the hardware configuration information for the machine.

Cancel
To close the window and not change the location of the device, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Support Element

Use this window to add a Support Element to the hardware configuration. Select a support element and the location of the Support Element as you want it identified in the hardware configuration, then click **Add Support Element**.

Machine type
Displays the machine type of the machine.

Machine model
Displays the model number of the machine.

Support Elements
Select a Support Element from this table, then select the location as you want it identified in the hardware configuration.

Available support element locations
Select a Support Element, then select from this table the location as you want it identified in the hardware configuration.

Serial number
Specify the serial number of the machine.

Add Support Element
To add the selected Support Element to your hardware configuration, click **Add Support Element**.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Support Element Details

Use this window to confirm the Support Elements listed by description, serial number, and location and associated with a specific CPC.

To confirm the support elements, click **OK**.

Support Element(s) table
This table displays the current Support Elements by description, serial number, and location.

Associated CPC
This is the Central Processor Complex (CPC) that the device is physically connected to.

The CPC you select becomes associated with the device. The hardware configuration information for a machine is stored on the Support Elements of its CPCs. A Support Element stores information only for its CPC and the devices associated with the CPC.

Associating a device with a CPC is necessary to identify the Support Element used for storing the device information, and to indicate the device is physically connected to the CPC. But associating a device with a CPC does not affect which CPCs can be configured to use the device.

OK
To confirm the Support Elements listed with the associated CPC, click **OK**.

Help
To display help for the current window, click **Help**.

Update Support Element

Use this window to select a Support Element you want updated in the hardware configuration of the specified machine, then click **Update Support Element...**.

Machine type
Displays the machine type of the machine.

Machine model
Displays the model number of the machine.

Associated CPC
Displays the central processor complex (CPC) that the device is physically connected to.

The CPC you select becomes associated with the device. The hardware configuration information for a machine is stored on the Support Elements of its CPCs. A Support Element stores information only for its CPC and the devices associated with the CPC.

Associating a device with a CPC is necessary to identify the Support Element used for storing the device information, and to indicate the device is physically connected to the CPC. But associating a device with a CPC does not affect which CPCs can be configured to use the device.

Current Support Element(s) table
This table displays current Support Elements by description, serial number, and location.

Select the Support Element you want updated in the hardware configuration of the specified machine, then click **Update Support Element...**.

Update Support Element...
To update the Support Element you selected, click **Update Support Element...**.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Update Support Element

Use this window to select a Support Element type you want to change in the hardware configuration of the specified machine, then select **Update Support Element**.

Note: Updates to this window will overwrite the current Support Element configuration data.

Current support element
Specifies the name of the current Support Element.

Serial number
Specifies the current serial number of the Fibre Trunk selected for updating.

Location

Specifies the current location of the Fibre Trunk selected for updating.

Support element types
This table displays the support element types for the machine specified.

Select one and update the machine serial number, then click **Update Support Element**.

Updated serial number
Use this field to update the machine serial number.

Note: Updating this field will overwrite the current Support Element configuration data.

Update Support Element
To update the support element you selected, click **Update Support Element**.

Note: Updates to this window will overwrite the current Support Element configuration data.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Delete Support Element

Use this window to delete a Support Element from the hardware configuration of the specified machine, then click **Delete Support Element**.

Machine type
Displays the machine type of the machine.

Machine model
Displays the model number of the machine.

Associated CPC
Displays the Central Processor Complex (CPC) that the device is physically connected to.

The CPC you select becomes associated with the device. The hardware configuration information for a machine is stored on the Support Elements of its CPCs. A Support Element stores information only for its CPC and the devices associated with the CPC.

Associating a device with a CPC is necessary to identify the Support Element used for storing the device information, and to indicate the device is physically connected to the CPC. But associating a device with a CPC does not affect which CPCs can be configured to use the device.

Current Support Element(s) table
This table displays current Support Elements by description, serial number, and location.

Select the Support Element you want deleted from the hardware configuration of the specified machine, then click **Delete Support Element**.

Delete Support Element
To delete the Support Element you selected, click **Delete Support Element**.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Fibre Trunk

Use this window to add Fibre trunks to the current hardware configuration for the machine.

Machine type
Displays the machine type of the machine.

Machine model
Displays the model number of the machine.

Fibre trunk locations
Select the location of the lower, left-hand corner of the Fibre Trunk.

Serial number
Specify the serial number of the Fibre Trunk.

Add Fibre Trunk
To add a Fibre Trunk to the system with the information currently displayed, click **Add Fibre Trunk**.

Note: This unit is not displayed graphically. In order to view the Fibre Trunk configuration at a later time, select **Update Fibre Trunk** from the list of options.

Note: Click **Save and Exit** on the **Edit Frame Layout** window to save the updated device information with the hardware configuration information for the machine.

Cancel
To close the window without adding a Fibre Trunk, click **Cancel**.

Help
To display help for the current window, click **Help**.

Update Fibre Trunk

Use this window to update Fibre Trunk information currently in the hardware configuration for the machine.

Machine type
Displays the machine type of the machine.

Machine model
Displays the model number of the machine.

Fibre trunk locations
Select the location and serial number that correspond to the Fibre Trunk you want to update.

Update Fibre Trunk...
To update the currently selected Fibre Trunk location or serial number, click **Update Fibre Trunk...**.

Note: Click **Save and Exit** on the **Edit Frame Layout** window to save the updated device information with the hardware configuration for the machine.

Cancel
To close the window without updating a Fibre Trunk, click **Cancel**.

Help
To display help for the current window, click **Help**.

Update Fibre Trunk

Use this window to update Fibre Trunk information currently in the hardware configuration for the machine.

Machine Type
Displays the machine type of the machine.

Machine Model
Displays the model number of the machine.

Current location
Specifies the current location of the Fibre Trunk selected for updating.

Current serial number
Specifies the current serial number of the Fibre Trunk selected for updating.

Fibre trunk locations
Select the location of the Fibre Trunk.

Serial number
Specify the serial number of the Fibre Trunk.

Update Fibre Trunk
To update the specified Fibre Trunk with the new data specified on this panel, click **Update Fibre Trunk**.

Note: Click **Save and Exit** on the **Edit Frame Layout** window to save the updated device information with the hardware configuration information for the machine.

Cancel
To close the window without updating a Fibre Trunk, click **Cancel**.

Help
To display help for the current window, click **Help**.

Delete Fibre Trunk

Use this window to delete Fibre Trunks from the current hardware configuration for the machine.

Machine type
Displays the machine type of the machine.

Machine model
Displays the model number of the machine.

Fibre Trunk locations
Select the location and serial number that correspond to the Fibre Trunk you want to remove.

Delete Fibre Trunk
To delete the currently selected Fibre Trunk from the system, click **Delete Fibre Trunk**.

Note: Click **Save and Exit** on the **Edit Frame Layout** window to save the updated device information with the hardware configuration information for the machine.

Cancel
To close the window without deleting a Fibre Trunk, click **Cancel**.

Help
To display help for the current window, click **Help**.

Devices mounted in rear of frame

This window displays the current devices mounted in the rear of the frame.

Edit LPAR Internal Code Change

Partition Internal Code Change

Use this window to type the number that identifies the partition internal code change you want to add.

Partition internal code changes are identified by a 4 digit decimal number from 0000 through 9999. This number is also the last four characters in the eight character name of the source file for the partition internal code change.

The source file must be named as follows:

- The first 4 characters of the file name must be IQZQ.
- The last 4 characters of the file name must be a number from 0000 through 9999.
  - Logical partition internal code changes have identifiers in the range from 0000 through 4999.
  - Coupling facility internal code changes have identifiers in the range from 5000 through 9999.
  - The file type must be TRM.

Change Identifier
Type the change identifier of the partition internal code change you want to add to the changes currently managed by this utility.

- Type an identifier in the range from 0000 through 4999 to add a logical partition internal code change.
- Type an identifier in the range from 5000 through 9999 to add a coupling facility internal code change.

OK
To add the change identifier to the current partition internal code changes, click **OK**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Enable Dynamic Partition Manager

Accessing the Enable Dynamic Partition Manager task

Use this task to enable **DPM** mode on your system.

Note: This task is available only on the Support Element of a system that was ordered with the Dynamic Partition Manager (DPM) feature.

To access this task, select either the **Tasks Index** or **Systems Management** node in the navigation pane.

- In the Tasks Index window, either scroll or search for the task by name.
- From the Systems Management window, open the Configuration task group in the tasks pad, and select the task.

Enable Dynamic Partition Manager

Use this task to enable Dynamic Partition Manager (DPM) for the system. You can use either the default SERVICE user ID or any customized user IDs that a system administrator has authorized to this task through customization controls in the **User Management** task.

Notes:

- This task is available only on the Support Element of a system that was ordered with the Dynamic Partition Manager (DPM) feature.
- Before you can use this disruptive task, you must deactivate the CPC first. During the DPM enablement process, the Support Element restarts to activate DPM code. After the DPM enablement process completes, apply the latest microcode control levels (MCLs) to make sure that the most recent DPM code is active on the Support Element before you begin using the DPM-enabled CPC.

  If any partitions (images) were defined while the CPC was running in standard mode (that is, with Processor Resource/System Manager or PR/SM), those definitions (profiles) are lost and must be recreated through the **New Partition** task.

To enable **DPM** mode on your system:

1. Select the system for which you want to enable **DPM** mode.
2. Open the **Enable Dynamic Partition Manager** task. The Enable Dynamic Partition Manager window is displayed.
3. Click **Enable** to perform the operation.

   Note: The Support Element will restart to complete the operation.

Additional functions on this window include:

Enable
To enable DPM for the system, click **Enable**.

Cancel
To close the window and confirm that DPM is not enabled, click **Cancel**.

Help
To display help for the current window, click **Help**.

Enable I/O Priority Queuing

Accessing the Enable I/O Priority Queuing task

This task allows you to enable or disable I/O priority queuing for the system. Enabling the I/O priority queuing allows the system to specify a priority to be associated with an I/O request at start subchannel time.

To enable or disable the I/O priority queuing:

1. Open the **Enable I/O Priority Queuing** task.

   The Enable Input/Output (I/O) Priority Queuing window displays.
2. Click the menu under **Settings** to make your selection:

   Enabled
   Activates I/O priority queuing for the CPC.

   Disabled
   Deactivates I/O priority queuing for the CPC.
3. Click **Save** to save the setting.

Enable Input/Output (I/O) Priority Queuing

Use this window to view or change global Input/Output (I/O) priority queuing current setting for the system. The possible settings are to enable I/O priority queuing or to disable I/O priority queuing.

I/O priority queuing, when enabled, allows the operating system to specify a priority to be associated with an I/O request at start subchannel time. A range of priorities for a logical partition will be supported. These values will be passed on to the I/O subsystem for use when making queuing decisions with multiple requests.

Enable Input/Output (I/O) Priority Queuing
Use this table to enable (or disable) I/O priority queuing dynamically after an Initial Microcode Load (IML).

I/O priority queuing allows the operating system to specify a priority to be associated with an I/O request at Start Subchannel time. These values are passed to the I/O subsystem for use when making queuing decisions with multiple requests.

Object Name
Displays the names of the CPCs in the group selected.

Setting
To enable I/O priority queuing for the CPC, select **Enabled**. To disable the I/O priority queuing for the CPC, select **Disabled**.

Save
To save the setting you selected, click **Save**.

Reset
To discard the unsaved changes made and display the initial settings, click **Reset**.

Cancel
To cancel your request to enable or disable I/O priority queuing, click **Cancel**.

Help
To display help for the current window, click **Help**.

Enable/Disable Dynamic Channel Subsystem

Accessing the Enable/Disable Dynamic Channel Subsystem task

Performing a power-on reset of the central processor complex (CPC), either directly or by activating the CPC, establishes many of its initial operational capabilities and characteristics, including whether dynamic input/output (I/O) configuration is enabled or disabled. After a power-on reset of the CPC is performed, changing its operational capabilities and characteristics requires performing another power-on reset.

If a power-on reset of the CPC initially enables dynamic I/O configuration, a task becomes available on the support element workplace for changing the CPC's dynamic I/O setting without performing another power-on reset.

To change the CPC's dynamic I/O setting without performing a power-on reset:

1. Open the **Enable/Disable Dynamic Channel Subsystem** task to start it.

   The Customize Dynamic Channel Subsystem window displays.
2. Use the window's controls, as follows, to enable or disable dynamic I/O for the CPC:
   a. Review the CPC's current setting for dynamic I/O. The selected **Enabled** or **Disabled**, indicates the current setting.
   b. While dynamic I/O is enabled, select **Disabled** to change the setting to disabled.
   c. Or while dynamic I/O is disabled, select **Enabled** to change the setting to enabled.
   d. Click **OK** to save the setting and close the window.

Enable or Disable Dynamic Channel Subsystem

Use this window to change the CPC's dynamic I/O setting *without* having to perform a power-on reset to make the new setting take effect.

Your input/output (I/O) configuration is the set of all I/O device, control units, and channel paths you define to your hardware and software.

Performing a power-on reset establishes the *hardware I/O definition*. That is, it defines the I/O configuration to the hardware. Loading the software establishes the *software I/O definition*. That is, it defines the I/O configuration to the software.

If the hardware and software support *dynamic I/O configuration*, you can change their I/O definitions dynamically. That is, changes made through dynamic I/O configuration take effect immediately; they do *not* require a power-on reset or load to make them take effect.

Performing a power-on reset of the CPC, either directly or by activating the CPC, establishes many of its initial operational capabilities and characteristics, including whether dynamic I/O is enabled or disabled. Ordinarily, after a power-on reset of the CPC is performed, changing its operational capabilities and characteristics requires performing another power-on reset. The **Enable/Disable Dynamic Channel Subsystem** task allows you to change the CPC's dynamic I/O setting *without* having to perform a power-on reset to make the new setting take effect.

Dynamic channel subsystem
This field indicates whether dynamic input/output configuration (dynamic I/O) currently is enabled or disabled for the central processor complex (CPC).

Select the new setting to change the setting, then click **OK** to make the new setting take effect. The settings are:

Enabled
To enable dynamic I/O, select this option.

Disabled
To disable dynamic I/O, select this option.

OK
To save the dynamic I/O setting currently selected, click **OK**.

Cancel
To end the task and undo any changes made to dynamic I/O, click **OK**.

Help
To display help for the current window, click **Help**.

Enabled/Disabled Setting

Enabled/Disabled Setting

Use the **Enabled** and **Disabled** settings for the **Automatic Activation** and **Enable I/O Priority Queuing** tasks.

Settings table
To enable the **Enable I/O Priority Queuing** or **Automatic Activation** tasks, select **Enabled**. To disable the tasks, select **Disabled**.

Save
To save the setting you selected, click **Save**.

Reset
To discard changes you made and display the current settings, click **Reset**.

Cancel
To cancel your request to enable or disable the **Enable I/O Priority Queuing** or **Automatic Activation** tasks, click **Cancel**.

Help
To display help for the current window, click **Help**.

Energy Optimization Advisor

Accessing the Energy Optimization task

Use this task to view recommendations that will reduce power consumption based on your present system operations. The task displays recommendations (advices) in graphical form. There are two types of power consumption you can manage; inlet air temperature and static power save mode.

Note: The messages are refreshed every 10 minutes. Relaunch this task to view the current messages.

1. Locate and open the **Energy Optimization Advisor** task. The Energy Optimization Advisor window displays.
2. Click the hyperlink in the Advice table to display thermal or utilization advice graphically for your system. You can optionally click the hyperlink to open the **Set Power Savings** task from the Processor Utilization Advice window.
3. Click **Close** to close the window.

Energy Optimization Advisor

This window displays recommendations that reduces power consumption based on the present system operation. Select the advice hyperlink to provide specific recommendations for your system.

Note: The messages are refreshed every 10 minutes. Relaunch this task to view the current messages.

The following list provides a description of each element in the Energy Optimization Advisor window:

Energy Optimization Advisor table toolbar

You can work with the table by using the table icons or **Actions** list from the Energy Optimization Advisor table tool bar.

Export

Export as HTML
Downloads table data into a Hypertext Markup Language (HTML) file. This action is only available when you are using a remote browser.

Export All to CSV
Downloads table data into a Coma Separated Values (CSV) file. You can then import the downloaded CSV file into most spreadsheet applications. This action is only available when you are using a remote browser.

Print

Print All
Prints all rows in the table. This action is only available when you are using a remote browser.

Print Selected
Prints selected rows in the table. This action is only available when you are using a remote browser.

Print Preview
Displays a printable version of all rows in the table. This action is only available when you are using a remote browser.

Configure Options
Provides a way to exclude or include specific columns from the table display. Available columns are in lists by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**

Columns in the Energy Optimization Advisor table

The following columns are displayed for the Energy Optimization Advisor table. You can modify the columns in the default table display by using the **Configure Options** icon.

“Thermal Advice” on page 583
Displays your system power consumption and inlet air temperatures graphically for each processor in the system.

“Processor Utilization Advice” on page 583
Displays your system processor utilization graphically and thermal advice.

Time and Date
Displays the time and date the advice was generated for your system.

Additional functions on this window include:

Close
To exit this task, click **Close**.

Help
To display help for the current window, click **Help**.

Thermal Advice

This window displays the power consumption and inlet air temperature graphically for your system and thermal advice. The graph displays the air inlet temperature on the left and the system power consumption on the right. The temperature threshold relevant to this recommendation is shown as a dashed horizontal line. Select the **Monitor Dashboard** link for real time trending data.

Select from the drop down list the time span for the x axis. Selecting a different time scale results in the chart re-rendering updating temperature and power consumption data on the span for the recommendation selected:

- Four hours
- One day
- Three days
- One week

Additional functions on this window include:

Close
To exit this task, click **Close**.

Help
To display help for the current window, click **Help**.

Processor Utilization Advice

This window displays the processor utilization graphically for each processor in the system. The graph displays the processor utilization as a percentage on the left side. The temperature threshold relevant to this recommendation is shown as a dashed horizontal line. Select the **Monitor Dashboard** link for real time trending data or **Set Power Savings** link to set the system into static power save mode.

Select from the drop down list the time span for the x axis. Selecting a different time scale results in the chart updating processor utilization for the recommendation selected:

- Four hours
- One day
- Three days
- One week

Additional functions on this window include:

Close
To exit this task, click **Close**.

Help
To display help for the current window, click **Help**.

Environmental Dashboard

Accessing the Environmental Dashboard task

To display system overview power graphically and power and environmental metrics chart:

1. Open the **Environmental Dashboard** task. The Environmental dashboard window is displayed.
2. Select the systems, partitions, and metrics from the drop-down menus to graphically display the power and environmental metrics.
3. Select a pre-defined time range or a set of custom time range from the drop-down menu to view the metrics.
4. Select Export to save the power and environmental metrics that is currently displayed to a Comma Separated Values (csv) file .
5. When you have completed this task, click **Close**.

Environmental dashboard

This Environmental dashboard window allows you to integrate new system and partition level power consumption metrics data, select time ranges for metric views for selected systems and partitions, display selected system and partition metrics in line chart and tabular views, and export metric data to a CSV format.

Environmental dashboard systems views:

Systems
Use the drop-down menu to select systems to view metrics in the System overview and the Power and environmental view.

System metrics
Use the drop-down menu to select the system metrics to view in the Power and environmental chart.

System overview
Displays graphically the overall total partition power, infrastructure power, and assigned power to all systems and each selected system.

Power and environmental metrics chart
Displays graphically the power and environmental metrics for the selected systems.

Environmental dashboard partitions views:

Partitions
Use the drop-down menu to select partitions to view their power and environmental metrics.

Partition metrics
Use the drop-down menu to select the partition metrics to display in the power and environmental chart.

Power and environmental metrics chart
Displays graphically the power and environmental metrics for the selected partitions.

Environmental dashboard time range and temperature views:

Time range
Use the Time-range drop-down menu to select a pre-defined time range or a set of custom time range to view the power and environmental metrics for a selected system or partition.

Temperature
Temperature metrics is enabled when a temperature-related metric is selected. The temperature is in Celsius and Fahrenheit (Default depending on location).

Additional functions on this window include:

Export
Select Export in the top right-hand corner to export the Environmental Dashboard Statistics data into a spread-sheet format.

Close
To close this window, click **Close**.

Help
To display help for the current window, click **Help**.

Export/Import Profile Data

Accessing the Export/Import Profile Data task

This task allows you to export or import activation profiles for the CPC to the hard drive, removable media, or FTP server. Exporting and importing profiles is necessary only when you intend to have your current system and Support Element replaced with a new system and Support Element. When a Capacity Backup Upgrade (CBU) is activated, more processors are activated in the system. In most cases, this requires you to change your activation profiles to include these new processors in the next activation. Otherwise, the CP/SAP split in the reset profile and the number of dedicated CPs/ICFs and other processor options in the Image profile won't specify the correct options.

To export/import profile data:

1. Open the **Export/Import Profile Data** task to start it.

   The Export/Import Profiles window displays.
2. Select the option you want to export or import profiles:
   - Export/import profiles to/from hard drive
   - Export/import profiles to/from removable media.
   - Export/import profiles via FTP Server

   Note: If you are using a USB flash memory drive, plug it into the console and then wait for the console to beep three times. This indicates that the device is ready and can be accessed. If it does not beep three times, unplug the device and try again. See the USB flash memory drive information.
3. Click **OK**.

Export/Import Profile Data

Use this window to select where to export or import activation profiles for the Central Processor Complex (CPC).

- To export or import profiles to/from hard drive, you must select “Hard drive” on page 586.
- To export or import profiles to or from a removable media, you must select “Removable media” on page 586.
- To export or import profiles to or from an FTP server, you must select “FTP Server” on page 587

Activation profiles are sets of information used to activate the CPC and its images.

Activation profiles are stored on the CPC's Support Element. Select where you want to export or import the profiles from, then click **OK** to start the operation.

OK
To export/import profiles to/from the selected drive, click **OK**.

Cancel
To close the window *without* importing or exporting any profiles, click **Cancel**.

Export/Import Profiles

Use this window to enter a description of the profile that you want to export or import. You can enter a 25 character description for the profile that you want to export or import.

OK
To export or import the file name, click **OK**.

Cancel
To close the window without exporting or importing a file, click **Cancel.**

Hard drive

The profiles are stored in a single file in a hard drive area controlled by the Licensed Internal Code (LIC). There are four areas on the hard drive to choose from. The file name cannot be specified. Select the area you want to export or import using the following display fields:

Date
Shows the date the data was previously exported to this area.

Time
Shows the time the data was previously exported to this area.

Description
Identifies the previously exported data.

These additional functions are available from this window:

Export to Hard Drive
To export the profiles to the selected hard drive area, click **Export to Hard Drive**.

Import from Hard Drive
To import the profiles from the selected hard drive area, click **Import from Hard Drive**.

Cancel
To close the window *without* importing or exporting any profiles, click **Cancel**.

Help
To display help for the current window, click **Help**.

Removable media

Use this window to export or import activation profiles for the Central Processor Complex (CPC) from a selected removable media.

Activation profiles are sets of information used to activate the CPC and its images.

Activation profiles are stored on the CPC's Support Element. For each type of profile:

- *Exporting* the profiles copies them from the Support Element to a removable media.
- *Importing* the profiles copies them from a removable media to the Support Element. The profiles are imported from a single *source file* on the removable media.

Select the types of profiles you want to export or import, and identify the operation's target file or source file. Then click **Export to removable media** or **Import from removable media** to start the operation.

These additional functions are available from this window:

Activation Profiles type
To export or import *all* activation profiles, check **Activation profiles**, then type the target file or source file name in the **File name** field.

Otherwise, if you do not want to export or import activation profiles, do not check **Activation profiles**.

Export to removable media
To export the profile to a removable media, click **Export to removable media**. This exports *all* profiles to its specified target file.

Import from removable media
To import the profile to a removable media, click **Import to removable media** This imports *all* profiles to its specified target.

Cancel
To close the window without importing or exporting any profiles, click **Cancel**.

Help
To display help for the current window, click **Help**.

Select Media Device

Use this window to copy data to/from the selected media.

Note: If you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message is displayed indicating the drive was not added and that you should remove the device and try again.

These additional functions are available from this window:

USB Flash Memory Drive
To use a USB flash memory drive as the media to copy data, select **USB Flash Memory Drive**.

OK
To confirm your request to copy data to/from the selected media, click **OK**.

Refresh
To redisplay the list of available media, click **Refresh**. Use this option if you did not insert your media before this point in the task.

Cancel
To close the window without importing or exporting any profiles, click **Cancel**.

Help
To display help for the current window, click **Help**.

FTP Server

Use this window to export or import activation profiles for the Central Processor Complex (CPC) from an FTP server.

Activation profiles are sets of information used to activate the CPC and its images.

Activation profiles are stored on the CPC's Support Element. For each type of profile:

- *Exporting* the profiles copies them from the Support Element to an FTP server.
- *Importing* the profiles copies them from an FTP server to the Support Element. The profiles are imported from a single *source file* on the FTP server.

The export function copies a source file from the Support Element to the FTP destination.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.

- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the Manage SSH Keys task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the file path and the file name of the zip file that is to be saved or read from.

Additional functions on this window include:

Export
To export a file to an FTP server, click **Export**.

Import
To import a file from an FTP server, click **Import**.

Cancel
To close the window without performing the selected operation, click **Cancel**.

Help
To display help for the current window, click **Help**.

FCP Configuration

Accessing the FCP Configuration task

The N Port Identifier Virtualization (NPIV) for Fibre Channel Protocol (FCP) channels allows sharing of a single physical FCP channel among operating system images. Use this task to display or alter worldwide port names assigned to FCP channels.

Use this task to:

- Display all N Port Identifier Virtualization (NPIV) port names currently assigned to FCP subchannels...
- Display WWPN for the physical ports of FCP channels...
- Import or export configuration...
- Release all port names that had previously been assigned to FCP subchannels that are now locked
- Release a subset of the port names that had previously been assigned to FCP subchannels that are now locked...
- Reset WWPN assignments for physical ports

To enable the NPIV mode for selected channel paths see the **FCP NPIV Mode On/Off** task.

To display or alter worldwide port names assigned to FCP channels:

1. Locate the **CPC** to work with.
2. Open the **FCP Configuration** task.

   The FCP Configuration window displays.
3. Select the operation you want to perform from the FCP Configuration window.
4. Click **OK** after making your selection.

FCP Configuration

This task allows you to display or alter worldwide part names assigned to FCP channels for the selected CPC.

When NPIV mode is enabled for selected logical partitions, the system provides a virtual FCP channel for each S/390® device definition for an FCP channel in the active input/output configuration.

Each virtual FCP channel is logged into the Storage Area Network (SAN) using a worldwide unique identifier. This worldwide port name (WWPN) is assigned by the system and used during the login procedure with the SAN when an operating system establishes a communication path to an FCP channel.

Use this FCP Configuration window to:

- Display all NPIV port names that are currently assigned to FCP subchannels...

  The “Display FCP NPIV Port Names” on page 590 window allows you to select what ports to display.
- Display WWPN for the physical ports of FCP channels...

  The “Display WWPN for the physical ports of FCP channels” on page 592 window displays the PCHID and corresponding WWPN.
- Import or export configuration...

  The “Import or Export Configuration” on page 589 window allows you to select an action and a location to export or import WWPN for physical ports.
- Release all port names that had previously been assigned to FCP subchannels and are now locked
- Release a subset of the port names that had previously been assigned to FCP subchannels and are now locked...
- Reset WWPN assignments for physical ports.

Additional functions on this window include:

Cancel
To exit this task, click **Cancel**.

OK
To continue with the operation, click **OK**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Display all NPIV port names that are currently assigned to FCP subchannels...

To display the worldwide port names assigned to FCP subchannels, select **Display all NPIV port names that are currently assigned to FCP subchannels...**.

Display WWPN for the physical ports of FCP channels...

To display the worldwide port names for the physical ports assigned to FCP channels, select **Display WWPN for the physical ports of FCP channels...**.

Import or Export Configuration

Use this window to select an action and location to export or import NPIV system or mode configuration file.

Action:

- Export binary NPIV system configuration file
- Export binary NPIV mode configuration file
- Export WWPN for physical ports
- Import binary NPIV system configuration file
- Import binary NPIV mode configuration file
- Import WWPN for physical ports.

Location:

- Hardware Management Console USB flash memory drive
- FTP site.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To exit this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Release all port names that had previously been assigned to FCP subchannels and are now locked...

To release and reassign all locked worldwide port names that had previously been assigned to FCP subchannels and are now locked, select **Release all port names that had previously been assigned to FCP subchannels and are now locked...**.

When NPIV mode is enabled for selected logical partitions, the system provides a virtual FCP channel for each S/390 device definition for a FCP channel in the active input/output configuration.

After a WWPN has been assigned to a virtual FCP channel and the S/390 device definition is deleted, the WWPN is not eligible for reassignment to a different virtual FCP channel. Rather, the WWPN and the virtual FCP channel are remembered in a least-recently used (LRU) list. If the same S/390 device definition is added back again, the same WWPN will be assigned to the pertaining virtual FCP channel.

Since the size of the LRU list is limited, the WWPN and the virtual FCP channel may be removed from the LRU list. The WWPN is then locked to prevent from reassignment to a different virtual FCP channel.

Use this window to release a subset of locked worldwide port names to make them available for assignment to different S/390 devices when WWPNs available for new virtual FCP channels become exhausted.

Release a subset of the port names that had previously been assigned to FCP subchannels and are now locked...

To release and reassign a subset of locked worldwide port names that had been previously assigned to FCP subchannels and are now locked, select **Release a subset of the port names that had previously been assigned to FCP subchannels and are now locked...**.

Display FCP NPIV Port Names

The selection list allows you to display all PCHID and/or LPAR assigned ports.

- Display all assigned ports
- Display all assigned ports for an LPAR
- Display all assigned ports for a PCHID.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To exit this task, click **Cancel**.

You can find more detailed help on the following elements of this window:

Display Assigned Port Names

Use this window to display the worldwide port names assigned to FCP subchannels.

Note: This window will not automatically refresh and therefore does not reflect any configuration changes while the window is open. You can transfer the information to a different server using the File Transfer Protocol (FTP) function on this window. This function may be useful when setting your Storage Area Network (SAN) configuration or devices attached to the SAN.

Select an option to:

- Show only entries defined with the current configuration
- Show only entries with NPIV On.

Additional functions on this window include:

Apply
To display information for the selected entry, click **Apply**.

Transfer via FTP
To export the worldwide port name assignment information into a file to transfer using FTP destination, click **Transfer via FTP**.

Cancel
To exit this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more help on the following elements of the Display Assigned Port Names window:

Display assigned port names table

Partition
Displays the name of the logical partitions.

CSS
Displays a number that identifies the channel subsystem a channel path is in.

ID
Displays the Image ID number that identifies the channel path.

CHPID
Displays a number that identifies the channel path identifier.

SSID
Displays the Subchannel Set ID for the channel path

Device Number
Displays a number that identifies a device.

WWPN
Displays the worldwide port numbers for the logical partitions.

NPIV Mode
Displays the NPIV mode for the logical partitions.

Current Configured
Displays whether the IOCDS for the logical partition is active.

PCHID selection

Select from the PCHID name list, the specific PCHID you want to display the assigned ports.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To exit this task, click **Cancel**.

LPAR selection

Select form the LPAR name list, the specific LPAR you want to display the assigned ports.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To exit the current window, click **Cancel**.

Display WWPN for the physical ports of FCP channels

This windows displays the physical channel identifier (PCHID) and corresponding worldwide port name for all FCP channels.

Additional functions on this window include:

Export to USB Flash Memory Drive

To export the WWPN view for the physical ports of FCP channels, click **Export to USB Flash Memory Drive**.

Notes:

- Available only from the Hardware Management Console.
- If you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message is displayed indicating the drive was not added and that you should remove the device and try again.

Cancel
To exit this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Release Subset

When NPIV mode is enabled for selected logical partitions, the system provides a virtual FCP channel for each S/390 device definition for a FCP channel in the active input/output configuration.

After a WWPN has been assigned to a virtual FCP channel and the S/390 device definition is deleted, the WWPN is not eligible for reassignment to a different virtual FCP channel. Rather, the WWPN and the virtual FCP channel are remembered in a least-recently used (LRU) list. If the same S/390 device definition is added back again, the same WWPN will be assigned to the pertaining virtual FCP channel.

Since the size of the LRU list is limited, the WWPN and the virtual FCP channel may be removed from the LRU list. The WWPN is then locked to prevent from reassignment to a different virtual FCP channel.

Use this window to release a subset of locked worldwide port names to make them available for assignment to different S/390 devices when WWPNs available for new virtual FCP channels become exhausted.

Additional functions on this window include:

Transfer via FTP
To export the worldwide port name assignment information into a file to transfer using FTP destination, click **Transfer via FTP**.

Release
To release the subset of worldwide port names that display on this window, click **Release**.

Cancel
To exit this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Import or Export Configuration

Use this window to select an action and location to export or import NPIV system or mode configuration file.

Action:

- Export binary NPIV system configuration file

- Export binary NPIV mode configuration file
- Export WWPN for physical ports
- Import binary NPIV system configuration file
- Import binary NPIV mode configuration file
- Import WWPN for physical ports.

Location:

- Hardware Management Console USB flash memory drive
- FTP site.

Additional functions on this window include:

OK
To continue with the operation, click **OK**.

Cancel
To exit this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

FCP NPIV Mode On/Off

Accessing the FCP NPIV Mode On/Off task

Use this task to enable N Port Identifier Virtualization (NPIV) mode for selected channel paths. When NPIV mode is enabled for selected channel paths, the system provides a virtual FCP channel for each S/390 device definition for a FCP channel in the active Input/Output configuration.

Note: The channel paths must be configured offline to enable NPIV mode.

To set the NPIV configuration:

1. Open the **FCP NPIV Mode On/Off** task.

   The NPIV Mode On/Off window displays.
2. Click **Select All** to select all the listed channel paths to enable for NPIV mode.
3. Click **Deselect All** to deselect all the listed channel paths that are enabled for NPIV mode.
4. Click **Apply** to make the changes.

FCP NPIV Mode On/Off

Use this window to enable FCP NPIV mode for selected channel paths. The channel paths must be configured offline to enable FCP NPIV mode.

FCP NPIV Mode On/Off table

This table contains the following information:

Partition
Displays the name of the logical partition.

CSS
Displays a number that identifies the channel subsystem a channel path is in.

CHPID
Displays a number that identifies the channel path identifier.

FCP NPIV Mode Enabled
Displays the FCP NPIV mode for the logical partition.

Select All
To select all the listed channel paths to be enabled for FCP NPIV mode, click **Select All**.

Deselect All
To deselect all the listed channel paths that are enabled for FCP NPIV mode, click **Deselect**.

Apply
To make the current changes to this window, click **Apply**.

Cancel
To cancel your request to enable FCP NPIV mode for selected channel paths, click **Cancel**.

Help
To display help for the current window, click **Help**.

File Transfer

File Transfer Information

To copy a configuration source file from the Support Element hard disk to a different medium.

Verify that the name in the **Source configuration** identifies the configuration that owns the source file you want to export.

Use the **Fully qualified file name** field to type the fully qualified name and extension of the file to receive the configuration source file on the FTP destination.

The export function copies a source file from the Support Element to the FTP destination.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the Manage SSH Keys task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

Additional functions on this window include:

OK
To perform the selected operation, click **OK**.

Cancel
To close the window without performing the selected operation, click **Cancel**.

Help
To display help for the current window, click **Help**.

Force Channel Internal Code Change

Accessing the Force Channel Internal Code Changes task

Internal code changes are pending for all channel, if any, that were busy during the most recent concurrent internal code change operation, and have remained busy since then.

The internal code change operation might have been either an installation and activation, or a temporary removal and activation of concurrent internal code changes. Rather than interrupting and ending activity on busy channels, their internal code was not updated, and the channel internal code changes were held pending for them.

When internal code changes are pending for one or more channel paths in the input/output (I/O) configuration of the central processor complex (CPC), you can forcibly update their licensed internal code with pending changes using the **Force Channel Internal Code Change** task.

Note: Forcibly updating the licensed internal code of a channel path interrupts and ends channel activity on busy channels that have internal code changes pending and might disrupt the operation of the CPC if it is using the interrupted channels.

To forcibly update licensed internal code with pending changes:

1. Open the **Force Channel Internal Code Change** task.

   The Force Channel Internal Code Change window displays.
2. Select the channels with changes pending that you want to force a licensed internal code update.
3. Click **Force** to forcibly update the licensed internal code of the channels with changes pending.

Force Channel Internal Code Update

When internal code changes are pending for one or more channel paths in the input/output (I/O) configuration of the central processor complex (CPC), this window identifies them by their channel path identifiers (CSS.CHPIDS) and allows you to forcibly update their licensed internal code with the pending changes. Otherwise, this window indicates there are no channel paths with pending internal code changes.

Important: Forcibly updating the licensed internal code of a channel path:

- Will interrupt and end channel activity on busy channels that have internal code changes pending.
- May disrupt the operation of the CPC if it is using the interrupted channels.

Note: See alternatives to forcibly updating internal code for information about actions you can take to update channel internal code with pending changes.

Channels with changes pending
Displays a list of channel path identifiers (CSS.CHPIDS) of channels with pending internal code changes.

Note: This list displays only when internal code changes are pending for one or more channel paths.

Force
To forcibly update the licensed internal code of the channels with changes pending, click **Force**.

Cancel
To close the window without updating the licensed internal code of the channels with changes pending, click **Cancel**.

Help
To display help for the current window, click **Help**.

Alternatives to forcibly updating internal code

The licensed internal code of busy channels will be updated with pending internal code changes under other conditions that may make forcibly updating the internal code unnecessary. The other conditions are:

- When channel activity stops
- During a power-on reset

The licensed internal code of busy channels will be updated with pending internal code changes when the channels are no longer busy. You can either:

- Use an operating system facility to end channel activity.
- Use tasks from the CHPID Operations task list of the Support Element workplace to end channel activity.

  Note: The operating system may not be notified when channel activity ends. For this reason, it is recommended you use an operating system facility, rather than the support element workplace, to end channel activity.
- Wait for channel activity to end.

  Note: This action may be impractical. Typically, channels with internal code changes pending are always busy.

The licensed internal code of busy channels will be updated with pending internal code changes when a power-on reset of the central processor complex (CPC) is performed.

Note: Activating the CPC is the recommended way to perform a power-on reset. You can use the **Activate** task from the Daily task list of the support element workplace to activate the CPC.

Channels with pending internal code changes

Internal code changes are pending for all channels, if any, that were busy during the most recent concurrent internal code change operation, and have remained busy since then.

The internal code change operation may have been either an installation and activation, or a removal and activation, of concurrent internal code changes. But rather than interrupting and ending activity on busy channels, their internal code was not updated, and the channel internal code changes were held pending for them.

Format Media

Accessing the Format Media task

Note: You cannot perform this task remotely.

Use this task to select the appropriate format type and file system for the removable media.

- Change management system update level
- Backup/restore
- Service data
- Upgrade data
- Security log
- Problem Analysis data
- User-specified label.

To format removable media:

1. Open the **Format Media** task. The Format Media window is displayed.
2. Select the format type for the removable media, make sure your media is properly inserted, then click **Format**. If you selected **User-specified label**, the Specify Label window is displayed. Specify a label, then click **Format**.
3. The Select Media Device window is displayed. Select the media you want to format, then click **OK**.

4. If you selected the USB flash memory drive, the Specify File System window is displayed. For all format types, except Backup/restore, select the file system (VFAT or EXT2) that you want to use to format the file on your USB flash memory drive, then click **Format**. Backup/restore defaults to the EXT2 file system.
5. When the media is formatted, the Format Media Completed window is displayed.

Format Media

Use this window to select the appropriate format type for the removable media.

Format	Label
"Change management system update level (ACTSUL)" on page 597	ACTSUL
"Backup/restore (ACTBKP)" on page 597	ACTBKP
"Service data (SRVDAT)" on page 597	SRVDAT
"Upgrade data (ACTUPG)" on page 597	ACTUPG
"Security log (ACTSECLG)" on page 597	ACTSECLG
"Problem Analysis data (VIRTRET)" on page 597	VIRTRET
"User specified label" on page 598	The label is automatically written to the removable media.

Change management system update level (ACTSUL)

This formatted removable media is used in the **Change Console Internal Code** task. To choose this format type, select **Change management system update level**.

Backup/restore (ACTBKP)

This formatted removable media is used in the **Backup Critical Console data** Hardware Management Console task. To choose this format type, select **Backup/restore**.

Service data (SRVDAT)

This formatted removable media is used in the **Transmit Service Data** task. To choose this format type, select **Service data**.

Upgrade data (ACTUPG)

This formatted removable media is used in the **Save Upgrade Data** task. To choose this format type, select **Upgrade data**.

Security log (ACTSECLG)

This formatted removable media is used in the **Archive Security Logs** task. To choose this format type, select **Security log**.

Problem Analysis data (VIRTRET)

This formatted removable media is used in the **Offload Problem Analysis Data to HMC Removable Media** task. To choose this format type, select **Problem Analysis data**.

User specified label

To specify your own label or leave blank, select **User specified label**. You can specify any label, up to 11 characters.

Additional functions are available from this window.

Format
To use the format type that you selected for your removable media, click **Format**.

If you selected **User specified label** and then clicked **Format**, the **Specify Label** window is displayed. You can type your own label name (up to 11 characters) in the **Label** input field or leave it blank. Click **Format** from that window to continue or **Cancel** to return to the previous window.

Cancel
To close this task without selecting a format type for the removable media, click **Cancel**.

Help
To display help for the current window, click **Help**.

Select Media Device

Use this window to select the desired removable media that is to be formatted.

Note: When you use a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

USB Flash Memory Drive
To use a USB flash memory drive as the removable media to be formatted, select **USB Flash Memory Drive**.

OK
To confirm your request to format the selected removable media, click **OK**.

Refresh
To redisplay the list of available removable media, click **Refresh**. Use this option if you did not insert your media before this point in the task.

Cancel
To close this window without formatting the removable media and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Specify File System

Use this window to select the appropriate file system you want to use to format the file on your USB flash memory drive.

VFAT
VFAT is the default file system for USB flash memory drives, it is supported on multiple operating systems, and has a maximum file size of 4GB. To use the virtual file allocation table (VFAT) file system to format the file on your USB flash memory drive, select **VFAT**.

EXT2
EXT2 is a LINUX file system that supports file sizes greater than 4GB on a USB flash memory drive. To use the second extended filesystem (ext2) file system to format the file on your USB flash memory drive, select **EXT2**.

Note: If you need to put any file greater than 4GB in size on your USB flash memory drive, then you can only use the EXT2 file system. If you choose **Backup/restore** as your format type, then this window is not displayed and the USB flash memory drive is formatted with the EXT2 file system.

Format
To format the file using the selected file system, click **Format**. A message window is displayed. You can continue with the operation by clicking **Yes** or you can return to the previous window by clicking **No**.

Cancel
To close this window without specifying a file system, click **Cancel**.

Help
To display help for the current window, click **Help**.

Grouping

Accessing the Grouping task

Managing groups enables you to create, delete, add to, and delete from user-defined groups of objects. You may want to create a group when you want to perform the same task on several images simultaneously instead of repeating the task on each individual image. This task also allows you to group one or more user-defined groups into other groups.

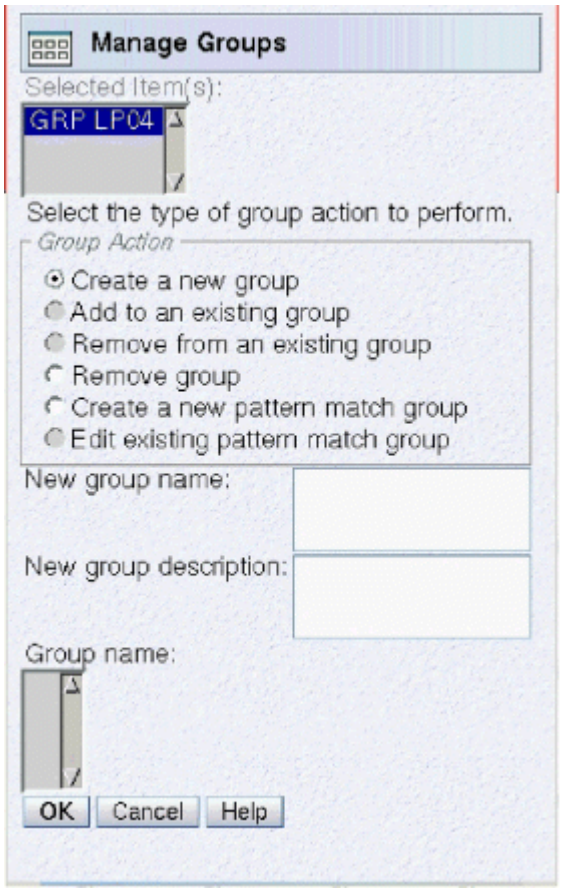


Figure 12. Creating a group

To group images:

1. Open the **Grouping** task. The Manage Groups window displays to allow you to add one or more selected objects to an existing group, delete one or more selected objects from a group, create a new group, create a pattern match group, or delete the group.

You might want to group one or more user-defined groups into other groups if you have many groups in your Groups Work Area and need additional work area space. However, if you group user-defined groups into other groups, you cannot perform any task other than **Grouping** on these groups.

To group groups of user-defined images:

1. Locate the **images** that you want to group.
2. Select one or more objects.
3. Open the **Grouping** task.

   The Manage Groups window displays.
4. Select **Create a new group** in the **Group Action** box.
5. Enter a *group name* in the **New group name** box.
6. Click **OK**. A **Create a New Group** window displays stating you successfully created a new group.
7. Click **OK**. The new group is now displayed in the Group Work Area.
8. Select another group that you want to add to the group you just created above.
9. Locate and start the **Grouping** task.

   The Grouping window displays.
10. Click *Add to an existing group* in the **Group Action** box.
11. Select the *group name* that you created in **step 9** above from the **Group Name** box.
12. Click **OK**. The Add to an Existing Group window displays that you have successfully added a group to another group.
13. Click **OK**. The group is no longer displayed in the Group Work Area because it is now part of the group you created in **step 9**.
14. Repeat **steps 11** through **14** for as many groups that you want to add to the new group.

Manage Groups

Use this task to create, delete, add to, or remove from user-defined groups of objects.

Select one or more groups to manage. You can then specify whether you want to create a new group, add to an existing group, or remove from an existing group.

Selected Item(s)
Lists the server(s) or group(s) you currently have selected.

Group Action
Select a grouping action to perform by using the selected managed objects:

- Create a new group
- Add to an existing group
- Remove from an existing group
- Remove group
- Edit an existing group
- Create a new pattern match group

Create a new group
To add the selected objects into a new group, select **Create a new group**, and specify a name in the New group field.

Add to an existing group
To add selected objects to a group, select **Add to an existing group**, and select a name from the Group name list.

Remove from an existing group
To remove the selected objects from a group, select **Remove from an existing group**, and select a name form the Group name list.

Remove group
To delete the user-defined group, select **Remove group**.

Edit existing group
To change the properties of an existing group, select **Edit existing group**, then click **OK** to continue.

Note: You cannot change the group name.

Create a new pattern match group
To create a group that contains objects of one or more specified types with names that match a specified pattern, select **Create a new pattern match group**, then click **OK** to continue.

New group name
Specify a name for a new group. This name, consisting of 1 to 30 characters, is required to create a new group.

New group description
Specify a description that represents this group name.

Group name
Displays the names for existing groups. Selecting a name from this list is required to add to or delete objects in a group.

OK
To accept the group actions, click **OK**.

Cancel
To exit this task without saving your changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Create/Edit Pattern Match Group

Use this window to create or edit a pattern match group.

- Select one or more group types from the list to be added to the pattern match group.
- Specify the name of the new group and specify a pattern to determine when a managed object is included in the group.

  Notes:

  – You cannot change the name of an existing group.
  – Once a pattern match group is defined and includes those objects that match the defined pattern, you cannot add additional objects to that group without changing the Managed resource pattern for that group.

Group type
Displays the names of managed object types that can be included in pattern matching groups.

Select the type of managed objects to include in the group. You can select more than one type by pressing Ctrl while selecting each item.

New group name
Specify a unique name for the new group. This is a required field, consisting of 1 to 30 characters.

New group description
Specify a description that represents this group name.

Managed Resource Pattern
Specify a pattern (expression) to use to determine whether a managed object of the specified type is included in the group. For example, if you specified **P0.***, this includes all objects whose name begins with **P0** and includes any number of characters that follow.

The pattern is applied to the name of the managed object, and the object becomes part of the group if the name matches the pattern.

OK
To accept the group information you provided, click **OK**.

Cancel
To exit this task without saving your changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Hardware Messages

Accessing Hardware Messages

The system and Support Element Console Application send messages to the support element console to notify you of significant events that involve or affect the use of system hardware and licensed internal code. The messages are referred to as *hardware messages*.

Hardware messages may be sent to the support element console at any time. The support element console receives the messages automatically, stores them in a message log, and turns on several console indicators to help you recognize that hardware messages were received.

The Support Element console can store a maximum of five hundred messages in its hardware message log. If the message log becomes full, the Support Element console continues to receive and store new messages, but deletes the log's oldest message for each new message that is received. Promptly view, act on, and delete hardware messages to avoid filling the message log and losing messages.

Viewing hardware messages

View hardware messages to remain informed of events that involve or affect the use of the system. Upon viewing hardware messages, you can also:

- Get more details for messages to determine what actions to take in response.
- Delete messages you no longer need.
- After you open the hardware messages notebook, use the online Help for more information on using it to view and delete hardware messages.

To get more details for messages:

1. Locate the system to work with.
2. Open the **Hardware Messages** task.
3. Select each message for which you want more details, then click **Details**.

   This opens a Details window, one at a time, for each selected message for which details are available.
4. Read the information and follow the directions on each details window to determine what action to take in response to a message. In many cases, you can use a details window itself to start the action.

Using hardware messages to report problems and get service

The system and Support Element Console Application send messages to the support element to notify you of significant events that involve or affect the use of system hardware and licensed internal code. The messages are referred to as *hardware messages*. Promptly view hardware messages as the Support Element receives them to determine their source and subject.

Problem Analysis issues hardware messages to notify you of problems detected by the Support Element. A hardware message issued by Problem Analysis typically is a brief, general description of a problem with hardware or licensed internal code. Information provided with the message includes a detailed description of the problem and instructions for either correcting the problem or reporting the problem and getting service.

Problem Analysis issues the hardware messages regardless of whether the Support Element's remote service settings are customized for automatically reporting problems and getting service. The remote service settings determine only how problem reports and service requests are transmitted:

- If remote service and automatic service calling are enabled, and if Problem Analysis determines service is required to correct a problem, it automatically transmits a problem report and service request to your service provider.

- If remote service or automatic service calling is not enabled, you must use the hardware message issued by Problem Analysis to report the problem and get service.

To use a hardware message to report a problem and get service:

1. Open the **Hardware Messages** task.

   The Hardware Messages window pages list the system's hardware messages and provides controls for working with them.

   Use the online Help for more information to view and delete hardware messages.
2. Select the message that describes the problem for which you want more details, then click **Details**.

   For hardware messages issued by Problem Analysis, this opens a Problem Analysis window that displays the message details.
3. Read the information and follow the directions on the Problem Analysis window to determine what action to take in response to the message.
4. If service is required to correct a problem, click **Request service** to report the problem to your service provider and to request service. The Support Element's remote service settings determine how the service request is made:
   - If remote service is enabled, requesting service transmits a problem report and service request to your service provider's automated service support system.
   - If remote service is not enabled, requesting service displays a window that provides all the information you need to call your service provider on the telephone, describe the problem, and request service.

Hardware Messages

This window displays messages about hardware activity for selected systems on this console.

A system's hardware messages notify you of events that involve or affect its hardware or internal code. For example, a hardware message for a system may indicate a hard error or internal code error occurred, or it may indicate Problem Analysis was performed.

To display the message for an system, select the name of that system that appears on the right side of the window. Messages are listed from the oldest to the newest message, with the oldest message displayed at the top of the list.

Tasks

All hardware messages awaiting operator action can be displayed for this system.

To promptly view, act on, and delete messages:

1. Select a message, then click **Details...** to display details.
2. If messages details are available and intervention is required, perform the operator action recommended in the details.
3. To delete the selected message, click **Delete**.

Note: This task may be view only for some user task roles.

Message Table
Messages are listed from the oldest to the newest message, with the oldest message displayed at the top of the list.

Date
Displays the date the message was sent.

Time
Displays the time the message was sent.

Message Text
Displays the message.

Details...
To display a further explanation of the hardware activity described by the message and a recommended operator action when intervention is required, for each selected message, click **Details...**.

Delete
To delete one or more selected messages from the list, click **Delete**.

Select All Messages
To select all messages listed, click **Select All Messages**.

Deselect All Messages
To deselect all messages listed, click **Deselect All Messages**.

Cancel
To close this window and cancel the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Messages awaiting operator action

A message is displayed until an operator action causes it to be deleted.

Some messages are deleted automatically after an operator displays the message or its details, if available. These messages generally provide information only, and are deleted automatically because no further action is required.

Messages that require further action provide message details that include a recommended operator action. The message and its details remain available until an operator deletes it manually. This allows reviewing the message details to assist operator intervention. But an operator must delete the message when its information is no longer required.

Deleting messages provides greater assurance of displaying new messages as they are received.

Image Details

Image Details

This window displays the current instance information, hypervisor information (if applicable), and acceptable status settings for the selected image.

An *image* is a set of Central Processor Complex (CPC) resources capable of running a control program or operating system. One or more images are created during a power-on reset of the CPC. Each logical partition is an image.

- Instance Information includes the current status of the image and other information about the image's operating conditions, characteristics, and settings.

  Review the information under **Instance information**. Optionally, click **Change Options...** to change the setting of the activation profile used for activating the image from the group specified in the **Group** field.

  Task information is information about the task performed most recently on the image.
- "Status" on page 607 settings determine which image statuses are acceptable and which statuses are unacceptable. The Support Element console reports when the image, CP, or channel path status becomes unacceptable.

  Review the settings on the **Status** page. Optionally, make setting selections and click **Apply** to change the acceptable status settings.

Apply
To save changes you made to the image's acceptable status settings, click **Apply**.

Change Options...
To change the setting of the activation profile used for activating this instance of the image from the selected group, click **Change Options**. You can have different activation profiles set for a single image

by invoking the **Image Details** task from different system defined or user-defined custom groups containing the object and selecting **Change Options...**.

The **Change Options...** button is not available if the **Image Details** task is invoked from Tasks Index. It is also not available if the user does not have permission to the **Change Object Options** task. Your access administrator can grant permission to the **Change Object Options** task by using the **User Management** task.

Cancel
To close the window without saving changes you made to the image's acceptable status settings, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more information on the Image Details tabs:

Instance Information

This page displays the current instance information for the selected image.

Instance information includes the current status of the image's central processors (CPs) and channel paths, and other information about the image's operating conditions, characteristics, and settings.

Group

Displays the name of the group that contains the instance of the image to which the instance information applies.

More than one group can contain a unique instance of the same image. This allows assigning different activation profiles to different instances of the image.

Note: The **Group** field is blank if the **Image Details** task is invoked from Tasks Index.

Image mode

Displays the mode set for the image.

Activation profile

Identifies the activation profile used for activating this instance of the image.

Optionally, click **Change Options...** to change the setting of the activation profile used for activating this instance of the image.

Note: The **Activation profile** field is blank if the **Image Details** task is invoked from Tasks Index.

Last used profile
Identifies the activation profile used for the most recent image activation.

Sysplex name

Displays the name of the particular operating system's complex (Sysplex).

A Sysplex is a collection of images that cooperate, using certain hardware and software products, to process workloads. If the image is running a particular operating system other than z/VM operating system, this field displays the name of the particular operating system's complex (Sysplex), if any, of which the image is a member.

System recovery boost
The System Recovery Boost provides the optional ability to allocate additional resource to have the system back and ready for work faster and catch up for lost time, without increasing monthly software costs.

- **Active boost class:** Values can be IPL, Shutdown, Recovery process boost, Not active, Not specified
- **Processor boost type:** Values are either Speed or zIIP and speed (Processor boost type field is hidden if there are no CP or zIIP processors being boosted)

- **Remaining zIIP recovery process boost time (mm:ss)** Value can be either 0 or a time between 00:01 and 30:00 (Remaining zIIP recovery process boost time field is hidden if there are no zIIP processors for the partition)
- **Remaining Speed recovery process boost time (mm:ss)** Value can be either 0 or a time between 00:01 and 30:00 (Remaining Speed recovery process boost time field is hidden if there are no CP processors for the partition)

Secure Execution for Linux
Indicates whether the selected image is using (On) or not using (Off) the Secure Execution installed feature.

VMSSI name

Displays the name of the particular Single System Image (SSI).

An SSI is a collection of images that cooperate, using certain hardware and software products, to process workloads. If the image is running a z/VM operating system (version 6.2), this field displays the name of the particular SSI, if any, of which the image is a member.

Group capacity name
Displays the group name that is assigned to the logical partition(s) in that group

Operating system name
Displays the name of the operating system, if available, currently loaded for the image.

CP management cluster name
Displays the CP cluster name of the selected image.

Simultaneous Multi-Threading (SMT)
Indicates if Simultaneous Multi-Threading (SMT) is active or inactive.

Operating system type
Displays the type of the operating system, if available, currently loaded for the image.

Operating system level
Displays the version and level of the operating system, if available, currently loaded for the image.

Include CP's in Standby state

Select a radio button to control how the CPs are summarized for the images status.

The default radio button for Include CPs in Standby State is to ignore CPs that are standby stopped. An image that contains CPs that are either operating or standby will have a summary status of Operating.

When the radio button to Include CPs in Standby State is selected, an image that contains CPs that are standby stopped will have a summary status of Exceptions.

- To include CPs in Standby state, click **Yes**. CPs that are standby stopped are not ignored and the summary status is Exceptions.
- To not include CPs in Standby state, click **No**. CPs that are standby stopped are ignored and the summary status is Operating.

To make the new setting(s) take affect, click **Apply**.

Lockout disruptive tasks

To set the disruptive task lockout for the image:

- To lock it (to prevent using the Support Element to perform disruptive tasks on the image), click **Yes**.
- To unlock it (to allow using the Support Element to perform disruptive tasks on the image), click **No**.
- Click **Apply** to make the new settings take effect.

Some Support Element tasks can be *disruptive*. Performing a disruptive task on the Central Processor Complex (CPC) or an image may disrupt its operations. For example, activating the CPC and loading an image can be disruptive.

Setting **Lock out disruptive tasks** controls whether you can perform disruptive tasks on an object. You can lock an object to prevent accidentally performing disruptive tasks on it, then unlock the object only when you want to perform a disruptive task on it.

Note: When you use the Support Element to set an object's disruptive task lockout, the setting affects only disruptive tasks that are started manually by console operators using the Support Element (locally or remotely) or Web server sessions. The setting does *not* affect disruptive tasks started automatically or from other sources. For example, the setting does not affect tasks started by scheduled operations, by Operations Management commands, or by console operators using the Hardware Management Consoles.

Validated boot certificates
Displays certificates that are assigned to the selected partition. If there are no certificates, *No certificates have been installed* displays.

Status

This page displays the current CP, CHPID, Crypto, and FID status and acceptable status settings for the image. **Acceptable status** settings determine which image, CP, CHPID, Crypto, and FID statuses are acceptable and which statuses are unacceptable.

Use the "Acceptable status" on page 609 check boxes to change the settings:

- A check mark in a check box indicates an acceptable status.
- An empty check box indicates an unacceptable status.
- To change one setting to the other, click once on the check box.

The Support Element continuously monitors the statuses of the image, CP, CHPID, Crypto, and FID, and compares them to the image's acceptable status settings.

You can find the status for the image, CP, CHPID, Crypto, and FID in the Status column of the image's work pane table.

Setting the image's acceptable status settings allows you to control which statuses are reported as exceptions:

- Acceptable status, indicated by check marks in their check boxes, are *not* reported as exceptions.
- Unacceptable status, indicated by empty check boxes, are reported as exceptions.

You can find more detailed help on the following elements of this page:

CP status

This field displays the current status of the central processor complex (CPC) or a summary of the statuses of its central processors (CPs).

Check stopped
All CPs are stopped due to machine checks.

No CPs are operating. Automatic error recovery failed or was not attempted.

Exceptions
At least one CP is operating, and at least one CP is not operating, but the exact statuses of the CPs vary.

Note: Use the CPC's pop-up menu to display the CPs and their exact statuses; instructions are provided below.

Loading
A load is in progress on all CPs.

No CPs are operating yet, but upon successful completion of the load, all CPs will be operating.

No power
CPC power is off.

CPs cannot operate until CPC power is turned on and a power-on reset is performed.

Not operating
If a power-on reset has not been performed: CPs cannot operate until a power-on reset of the CPC is performed.

If a power-on reset was performed: no CPs are operating, but the exact statuses of the CPs vary.

Note: Use the CPC's pop-up menu to display the CPs and their exact statuses; instructions are provided below.

Operating
All CPs are operating.

Recovering
Automatic error recovery is in progress on all CPs.

No CPs are operating, but upon successful recovery from the error, CPs will return to their previous statuses.

Otherwise, if error recovery is not successful, CPs will be check stopped.

Reset active
A reset is in progress on all CPs.

Upon successful completion of the reset, CPs will be stopped. No CPs will be operating yet, but they will be ready for loading.

Service Required
The CPC is still operating but is using the last redundant part of a particular type. Your CPC is shipped with more than the required number of parts to operate the CPC. You now have only the required number of parts to keep the CPC running. This is a reminder to you and your service representative that repairs should be made at the earliest possible time before additional parts fail that would make your CPC non-operating.

Status check
The CPC is not communicating with the support element.

The status of the CPs cannot be determined.

Stepping
All CPs are operating, but with their operation rates set to instruction step.

Each CP will be stopped after processing one instruction or one unit of instructions.

Stopped
All CPs are stopped.

If a reset completed successfully: no CPs are operating yet, but they are ready for loading.

If all CPs were stopped manually: no CPs are operating, but they can be started again at any time. Use the **Start all** workplace task to start all CPs at once, or use the **Start** task to start CPs individually.

CHPID status

This field displays the current summary of the statuses of CHPIDs of the central processor complex (CPC).

Acceptable
All CHPIDs are not operating, but their statuses are acceptable.

The exact statuses of the CHPIDs vary.

Exceptions
At least one CHPID is operating, but at least one CHPID is not operating.

The exact statuses of the CHPIDs vary.

Not operating
All CHPIDs are not operating and their statuses are unacceptable.

The exact statuses of the CHPIDs vary.

Operating
All CHPIDs are operating.

Crypto status

This field displays the current summary of the statuses for Crypto of the central processor complex (CPC).

Acceptable
All Crypto are not operating, but their statuses are acceptable.

The exact statuses of the Crypto vary.

Stopped
At least one Crypto is operating, but at least one Crypto is not operating.

The exact statuses of the Crypto vary.

FID status

This field displays the current summary of the statuses of FIDs of the central processor complex (CPC).

Acceptable
All FIDs are not operating, but their statuses are acceptable.

The exact statuses of the FIDs vary.

Check stopped
At least one FID is operating, but at least one FID is not operating.

The exact statuses of the FIDs vary.

Acceptable status

This field specifies which statuses are acceptable for the image. Select the statuses you want as acceptable. Then click **Apply** to save your changes and update the image status.

Operating
This term indicates the status of the image or the summarized status of its central processors (CPs) and channel paths.

Image status or summarized status of CPs: All CPs are operating.

Summarized status of channel paths: All channel paths are operating.

Not operating
This term indicates the status of the image or the summarized status of its central processors (CPs) and channel paths.

Image status or summarized status of CPs:

- No CPs are operating, but the exact statuses of the CPs vary.
- The following CP statuses are summarized as not operating:
  - Check stopped
  - Loading
  - Recovering
  - Reset active
  - Stepping
  - Stopped

Summarized status of channel paths: The following channel path statuses can be summarized as not operating:

- Bit error threshold exceeded

- Check stop
- Definition error
- Disabled
- I/O suppressed
- IFCC threshold exceeded
- Loading
- Log stored
- Loss of signal
- Loss of synchronization
- Match
- No power
- Not defined
- Not operational link
- Offline signal received
- Permanent error
- Sequence not permitted
- Sequence time-out
- Service
- Suspended
- Swapped
- Terminal condition
- Test mode
- Wrap block

Note: Each channel paths settings determine whether the channel paths statuses are summarized as not operating or acceptable.

Acceptable
This term indicates the summarized status of the channel paths.

Summarized status of channel paths: All channel paths are not operating, but with statuses that are acceptable; the exact statuses of the channel paths vary.

- Bit error threshold exceeded
- Check stop
- Definition error
- Disabled
- I/O suppressed
- IFCC threshold exceeded
- Loading
- Log stored
- Loss of signal
- Loss of synchronization
- Match
- No power
- Not defined
- Not operational link
- Offline signal received

- Permanent error
- Sequence not permitted
- Sequence time-out
- Service
- Suspended
- Swapped
- Terminal condition
- Test mode
- Wrap block

Note: The Support Element settings determine whether the channel paths statuses are summarized as not operating or acceptable.

Exceptions
This term indicates the status of the image or the summarized status of its central processors (CPs) and channel paths.

Image status or summarized status of CPs: At least one CP is operating, but at least one CP is not operating.

Summarized status of channel paths: At least one channel path is operating, but at least one channel path is not operating.

Not activated
This term indicates the status of the image or the summarized status of its central processors (CPs) and channel paths.

Image status or summarized status of CPs: The image is not activated.

Summarized status of channel paths: This status indicates image status only; it is not applicable to channel paths.

Save as default

To allow you to change the acceptable status for all of the current objects defined with the same status type, select **Save as default**. After you click **Apply**, a message window appears confirming that you want to proceed with this operation.

Test Mode

This page displays the test mode conditions for one or more central processors (CPs). Test mode is active when one or more of the following conditions are in effect:

Address compare is enabled
Indicates at least one active CP address match or input/output I/O) address match is set for stopping all CPs if an address match occurs.

Test mode will remain active under this condition until the active address matches are no longer active.

Checkout tests active
Indicates the **Checkout Tests** task is active and is either loading or running checkout tests.

Test mode will remain active under this condition until the checkout tests are completed or cancelled. Open the **Active Tasks** view, if necessary, to locate and restore the Checkout Tests Progress window, then either:

- Wait for the window to indicate the tests are complete
- Or, click **Cancel** from the window to cancel the tests.

Instruction stepping is enabled
Test mode will remain active under this condition until the operation rate of each affected CP is set back to *progressing*. Use the **Change Operation Rate** task to set a CPs operation rate.

I/O tracing is enabled
Indicates one or more input/output (I/O trace options are enabled for all CPs.

Test mode will remain active under this condition until all enabled I/O trace options are disabled. Use the **Trace** task to disable I/O trace options.

PSW I/O event compare is enabled
Indicates at least one PSW event or I/O event is set for stopping all CPs if an event occurs.

Test mode will remain active under this condition until the events are no longer enabled. Use the **Stop on PSW Event** or **Stop on I/O event** tasks to undo enabled PSW events or I/O events, respectively.

PSW tracing is enabled
Indicates one or more program status word (PSW) trace options are enabled for all CPs.

Test mode will remain active under this condition until all enabled PSW trace options are disabled. Use the **Trace** task to disable PSW trace options.

Click **Cancel** to close the window after reviewing the conditions.

Note: This page lists the conditions for which test mode is active at the time the page was opened. The conditions may change while the page is displayed, but the list will *not* be updated until you close the page then open it again.

Input/Output (I/O) Configuration

Accessing the Input/Output (I/O) Configuration task

The input/output (I/O) configuration of the central processor complex (CPC) is the set of all I/O devices, control units, and channel paths available to the CPC. During each power-on reset of the CPC, an input/output configuration data set (IOCDS) is used to define the I/O configuration to the channel subsystem.

You must build an IOCDS and store it on the CPC's Support Element before you can use it during power-on reset to define the CPC's I/O configuration. You can build an IOCDS by using an input/output configuration program (IOCP):

- An IOCP may be available as a batch program with your operating system.

  For information about using the IOCP, see: *Input/Output Configuration Program User's Guide for ICP IOCP*.
- A stand-alone IOCP also is available with the Support Element.

  For information about using the stand-alone IOCP, see: *Stand-Alone Input/Output Configuration Program User's Guide*.

This task allows you to start the support processor input/output configuration program (IOCP) for the selected CPC.

To start the stand-alone IOCP:

1. Open the **Input/output (I/O) Configuration** task.

   The Input/Output Configuration window displays.
2. Click **Options** from the menu bar to display the following menu options:
   - Enable Write Protection
   - Disable Write Protection
   - Copy Configuration
   - Export Source File
   - Import Source File

- Open Source File
- Delete Source File
- Print Data Set Report
- Write Report to Tape
- Build Data Set
- Disassemble Data Set.

3. Click **View** from the menu bar to display the following menu options:
   - Channel Path Configuration
   - Partition Images Configured
   - Dynamic Information
   - Configuration Program Level
   - Support I/O Mask.
4. Click **Tools** (Service role only) from the menu bar to display the following menu options:
   - Save Data Files on Hardware Management Console...
   - Save Data Files to USB Flash Memory Drive
   - Restore Data Files from Hardware Management Console...
   - Restore Data Files from the USB Flash Memory Drive...
   - Restore only IOCDS Data Files from USB Flash Memory Drive
   - Restore Only Channel Configuration Files from USB Flash Memory Drive
   - Erase Data Files from Hardware Management Console.
5. Click Exit from the **Options** menu bar to exit the window.

Input/Output Configuration

Use the **Input/Output Configuration** window to manage and modify input/output (I/O) configuration source files and data sets for the selected central processor complex (CPC). Use this window also to display information that defines the channel paths and logical partitions associated with the I/O configurations, and the status of configuration source files and data sets.

A configuration source file and an input/output configuration data set (IOCDS) are associated with each I/O configuration.

The source file is the input to the stand-alone I/O configuration program (IOCP). The IOCP uses a configuration source file to create or build an IOCDS.

The IOCDS is used during a power-on reset to define the I/O configuration program for the channel subsystem. The **Active input/output configuration data set (IOCDS)** field identifies the IOCDS used during the most recent power-on reset or selected by a dynamic activation from an operating system.

The **IOCDS matching hardware system area (HSA)** section displays the identifier of the IOCDS, if any, that matches the source most recently used to dynamically create the I/O definition currently in the channel subsystem HSA of the selected CPC, and then written to its support element. That is, the field identifies an IOCDS that supports dynamically changing the I/O definition defined by the IOCDS.

Note: If the I/O definition most recently created in the HSA was not written to the support element, then it may not match the I/O definition of the IOCDS identified by this field.

Click **Options** on the menu bar. The actions available for managing and modifying configuration files and data sets are listed below. Select an action from the following list:

"Enable Write Protection" on page 615
"Disable Write Protection" on page 616
"Copy Configuration" on page 616
"Export Source File" on page 616

"Import Source File" on page 617
"Export to HMC USB Flash Memory Drive" on page 618
Open Source File to edit the selected I/O configuration source file
Delete Source File to delete the selected I/O configuration file
"Print to printer" on page 619
"Write Report to Tape" on page 619
"Build Data Set" on page 620
"Disassemble Data Set" on page 621

Click **View** on the menu bar. The actions available for displaying information and status are listed below. Select an action from the following list:

"Channel Path Configuration" on page 621
"Partition Images Configured" on page 633
"Dynamic Information" on page 633
Configuration Program Level to display the version, release, and level of the stand-alone IOCP available on your Support Element .
"Supported I/O Mask" on page 634

Click **Tools** on the menu bar. The actions available for saving and restoring data files on the Hardware Management Console are listed below. Select an action from the following list:

"Save Data Files on Hardware Management Console" on page 634
Save Data Files to USB Flash Memory Drive to copy the IOCDS data files and channel configuration files from the Support Element console to the USB Flash Memory Drive
"Restore Data Files on Hardware Management Console" on page 635
Restore Data Files from the USB Flash Memory Drive to restore the IOCDS data files and channel configuration files from the Support Element console to the USB Flash Memory Drive
Restore only IOCDS Data File from USB Flash Memory Driveto restore only IOCDS data files from the Support Element console to the USB Flash Memory Drive
Restore only Channel Configuration Data File from USB Flash Memory Drive to restore only the channel configuration files from the Support Element console to the USB Flash Memory Drive
Erase Data File from Hardware Management Console to erase the IOCDS data file from the Hardware Management Console's hard drive. The fully qualified path name for the data files must be specified at the Target path name entry field.

You can find more detailed help on the following element of this window:

I/O configuration table

Select an input/output (I/O) configuration data set (IOCDS) to work on from the list. The list provides the following information about each data set:

Data Set
Displays the two-character identifier of an IOCDS. There are 5 data sets (A0, A1, A2, A3, and D0).

Name
Displays the eight-character name of an IOCDS. This name primarily identifies the data set to users, while the data set identifier is used by the system.

A data set name is specified by the first eight characters from the **MSG1=** keyword of the **ID** statement in the configuration source file.

Write Protected
Indicates whether write protection is enabled for the IOCDS. Enabled write protection prevents the IOCDS from being overlaid with a new IOCDS written by batch or the stand-alone IOCP.

No
Indicates write protection is disabled.

Yes
Indicates write protection is enabled.

Date
Displays the month, day, and year that the IOCDS was built.

Time
Displays the hour, minute, and second (continental time) that the IOCDS was built on the indicated date.

Data Set Status
Indicates the status of the I/O configuration data set.

Active
Indicates the data set was used during the most recent power-on reset or was selected by a dynamic activation from an operating system.

Valid
Indicates the data set contains no errors and can be used at power-on reset.

Invalid
Indicates the data set is not usable at power-on reset. This occurs when IOCP is currently writing to the IOCDS or the IOCDS was written in preparation for a CPC upgrade and will be unusable until the CPC is upgraded to the type of CPC supported by the IOCDS.

Source Status
Indicates the status of the I/O configuration data set source that is used in the build process by the stand-alone IOCP.

Empty
Indicates no source. This occurs when you delete the source file and when batch IOCP writes an IOCDS.

Imported
Indicates the source file was imported from the USB flash memory drive or FTP.

Modified
Indicates the source file has been changed by the editor.

Verified
Indicates the source file has no errors from the build process.

Warnings
Indicates the source file has warning or caution messages from the build process.

Errors
Indicates the source file has error messages from the build process. No IOCDS is written and the IOCDS remains as it was before the build.

Unknown
Indicates an error condition.

Version
Indicates the version of the IOCP that built the data set.

Enable Write Protection

Select **Enable Write Protection** to prevent modification of the selected input/output configuration data set (IOCDS) and the configuration source file.

With write protection enabled, the IOCDS cannot be modified using the build function of the input/output configuration program (IOCP), and the IOCDS cannot belong to the target configuration of the copy function. With write protection enabled, the configuration source file cannot be the target of the following functions:

- copy configuration
- import source
- open source
- delete source
- build

- disassemble

Disable Write Protection

Select **Disable Write Protection** to allow modification of the selected input/output configuration data set (IOCDS) and the configuration source file.

With write protection disabled, the IOCDS may be modified using the build function of the input/output configuration program (IOCP), and the IOCDS can belong to the target configuration of the copy function.

With write protection disabled, the source file may be modified using the open function, and the source file can be the target of the import or disassemble function or belong to the target configuration of the copy function.

Copy Configuration

Select **Copy Configuration** to copy an input/output (I/O) configuration.

The copy function duplicates the source file and the input/output configuration data set (IOCDS) of the source configuration and replaces the corresponding files of the target configuration. The target I/O configuration cannot be write-protected.

Source Configuration
Displays the identifier of the source configuration data set

Target Configuration
Select the identifier of the target configuration data set.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Export Source File

Select **Export Source File** to export a configuration source file from the Support Element hard disk to an FTP destination.

The export function copies a source file from the Support Element to an FTP destination.

Verify that the name in the **Source configuration** identifies the configuration that owns the source file you want to export.

Use the **Protocol** field to specify a secure network protocol for transferring files to the specified FTP destination. Use the **File path** field to type the file path directory where the files are to be saved or read.

Source configuration data set
Displays the identifier of the source configuration data set.

Source configuration data set name
Displays the name of the source configuration data set.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Export** drop-down, select **From Remote Server**. The Export Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Export window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

Additional functions on this window include:

Export
To export configuration data files to an FTP destination, click **Export**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Import Source File

Select **Import Source File** to copy a configuration source file from one medium to the Support Element.

The import function copies a source file from the FTP destination to the Support Element hard disk.

Use the **Protocol** field to select a secure network protocol for transferring files to the specified FTP destination. Use the **File path** field to type the file path directory where the files are to be saved or read.

Target configuration data set
Displays the identifier of the target configuration data set

Target configuration data set name
Displays the name of the target configuration data set

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then

click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.

- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

Additional functions on this window include:

Import
To import data configuration files to an FTP destination, click **Import**.

Cancel
To close the window without saving your changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

Export to HMC USB Flash Memory Drive

Select **Export Source File** to export a configuration source file from the Support Element hard disk to a USB Flash Memory Drive destination.

The export function copies a source file from the Support Element to a USB Flash Memory Drive destination.

Verify that the name in the **Source configuration** identifies the configuration that owns the source file you want to export. Use the **Target File name** field to type the fully qualified name and extension of the file to receive the configuration source file on the USB Flash Memory Drive.

Source configuration data set
Displays the identifier of the source configuration data set.

Source configuration data set name
Displays the name of the source configuration data set.

Target file name

Specify the fully qualified file name for the target file. For example:

```
DriveDirectoryfilename.ext
```

Additional functions on this window include:

OK
To export configuration data files to a HMC USB Flash Memory Drive destination, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Import to HMC USB Flash Memory Drive

Select **Import Source File** to import a configuration source file to the Support Element hard disk from a USB Flash Memory Drive destination.

The import function copies a source file to the Support Element to a USB Flash Memory drive destination.

Verify that the name in the **Source configuration** identifies the configuration that owns the source file you want to export. Use the **Target File name** field to type the fully qualified name and extension of the file to receive the configuration source file on the USB flash memory drive.

Source configuration data set
Displays the identifier of the source configuration data set.

Source configuration data set name
Displays the name of the source configuration data set.

Target file name

Specify the fully qualified file name for the target file. For example:

```
DriveDirectoryfilename.ext
```

Additional functions on this window include:

OK
To import configuration data files from a HMC USB Flash Memory Drive destination, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Print to printer

Select **Print to Printer** to specify the options necessary to print a configuration report.

This function works only with printers that accept standard line printer commands.

You must specify the device number of the printer, the number of lines to print per page, and whether to end the process upon a data check error. The printer must be a channel-attached device and must be in the active IOCDS and must be available to the logical partition you are using to run IOCP.

Use **Continue if data check errors occur** to indicate whether you want to stop printing if the printer receives a character that cannot be printed. A printer cannot print characters that are not recognized, or are not in the printer character set. Select this option if you want data check errors ignored. Otherwise, leave this selection blank.

Printer address
Specify the device number of the printer you want to use in the field. The printer's device number must be configured in the active IOCDS. The active IOCDS is the one that matches the current I/O configuration of the central processor complex (CC).

Lines per page
Specify the maximum number of lines printed on each page. The default value for this field is 55 lines per page. The IOCP uses the default value if the field is blank. The IOCP uses a value of 20 if you specify a value less than 20.

Continue if data check erros occur
To continue printing even with data check errors, click **Continue if data check errors occur**. When a character that cannot be printed is received, it is replaced with a blank and printing continues.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected functions, click **Cancel.**

Help
To display help for the current window, click **Help**.

Write Report to Tape

Select **Write Report to Tape** to specify the options necessary to write a formatted I/O configuration report to tape.

You must specify the device number of the tape drive, the file number location for the file on the tape, and the number of lines to include per page of the configuration report. The tape drive must be a channel-attached device and must be in the active IOCDS and must be available to the logical partition you are using to run IOCP.

Tape drive address
Specify the device number of the tape drive you want to use in the field. The device number must be configured in the active IOCDS. The active IOCDS is the one that matches the current I/O configuration of the central processor complex (CPC).

File number
Specify the number of the physical file on the tape (such as 1,2, or 3) where you want to store the file. IOCP issues a Rewind command followed by forward space file commands to position the tape to the requested file.

Lines per page
Specify the maximum number of lines to include per page of the I/O configuration report. The default value for this field is 55 lines per page. The IOCP uses the default value if the field is blank. The IOCP uses a value of 20 if you specify a value less than 20.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without saving your changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

Build Data Set

Select **Build Data Set** to run the stand-alone input/output configuration program (IOCP) and create an input/output configuration data set (IOCDS).

Note: This action cannot be used with an input/output (I/O) configuration that is write-protected.

The IOCP will build the IOCDS from the statements in the source file associated with the selected I/O configuration. The IOCP checks the syntax of the source file statements and validates the source file information. The IOCP imbeds error messages in the source file upon detecting errors.

If no terminal errors are encountered, the IOCP writes the IOCDS to the Support Element hard disk. Otherwise, edit the source file to correct the errors if it is not a dynamic I/O configuration. Conditions that result in warning or caution messages from the IOCP will not cancel the build.

If you select the option to print a report of the built IOCDS on a system printer, the system printer must be configured in the active IOCDS and available to the logical partition you are using to run IOCP.

Send output to printer
To send the report of the built IOCDS to the system printer select **Send output to printer**. The system printer must be configured in the active IOCDS and available to the logical partition you are using to run the IOCP.

Printer address
Specify the device number of the printer you want to use in this field. The printer's device number must be configured in the active IOCDS. The active IOCDS is the one that matches the current I/O configuration of the central processor complex (CPC).

Lines per page
Specify the maximum number of lines printed on each page. The default value for this field is 55 lines per page. The IOCP uses the default value if the field is blank. The IOCP uses a value of 20 if you specify a value less than 20.

Continue if data check error occur
To continue the build even with data check errors, select **Continue if data check errors occur**. When a character that cannot be printed is received, it is replaced with a blank and printing continues.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Input/Output Configuration Progress

The **Input/Output Configuration** window indicates the progress of the requested stand-alone IOCP task.

Start time
Displays the time at which the task begun

Elapsed time
Displays the amount of time that has elapsed since the task began

Current step
Displays the current step number being performed

Total number of steps
Displays the number of steps to be performed for the requested task

Status messages
Displays messages indicating the step being performed and the final result of the requested task

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Disassemble Data Set

Select **Disassemble Data Set** to run the stand-alone IOCP to generate a new I/O configuration source file based on the selected IOCDS. The new source file contains the full configuration described in the original customer IOCP input file and is the logical equivalent of the input file. However, it will not appear as it did in the original. Since IOCP does not save comments, comments do not appear in the source file.

Channel Path Configuration

Use the **Channel Path Configuration** window to select a channel path and the type of channel path information you want to view. The Channel path configuration table lists the channel paths that exist in the selected IOCDS.

Select a channel path, then select an action to display the type of channel path information you want to view. You can display information for control units or input/output (I/O) devices assigned to the channel path, or for names of logical partitions that have access to the path.

Click **View** on the menu bar. The actions available for displaying information are listed below. Select an action from the following list:

“Channel Subsystem Information” on page 624
“CHPID Information” on page 627
“Control Unit Information” on page 628
“Device Information” on page 629
“Image Candidate List” on page 630
“Image Access List” on page 631

Click **Search** on the menu bar. The actions available for searching information are listed below. Select an action from the following list:

"PCHID" on page 623
"CSS.CHPID" on page 623

The channel path information displayed is associated with keywords on the IOCP CHPID statement. The CHPID statement defines the characteristics of a channel path.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing.

You can find more detailed help on the following elements of this window:

Channel path configuration table

Select a channel path from the list to view more information about the channel path including the control units and devices assigned to the channel path.

PCHID=
The PCHID keyword identifies the physical channel identification number, if any, associated with the channel path.

TYPE=
The TYPE keyword identifies the mode of input/output (I/O) operation for the channel path.

CSS
The CSS parameter indicates the channel subsystems a channel path is in. This parameter is set in the PATH keyword of a CHPID statement. If a channel path is in multiple channel subsystems and therefore defined as spanned, **SPAN** is displayed. To display the specific channel subsystems a spanned channel path is in, use the Channel Subsystem Information view.

CHPID
This number identifies the channel path identifier. A channel path identifier is assigned by the PATH keyword of a CHPID statement.

SWITCH=
The SWITCH keyword identifies a number, if any, associated with an ESCON Director or FICON Director to support dynamic connections of the corresponding channel path identifier through the Director. It is valid for ESCON and FICON channel types only.

CHPARM=
The CHPARM keyword indicates how the channel path is to operate. Only certain channel path types support CHPARM. Also, for some channel path types that support CHPARM, only non-zero values are displayed.

PNETID
Displays the physical network identifier for the channel path.

TYPE keyword

The TYPE keyword identifies the mode of input/output (I/O) operation for the channel path.

A channel path may operate in one of the following modes:

CBY
Indicates a channel attached to an ESCON converter and operating in byte multiplexer mode. CBY channel paths operate the same as parallel channels operating in byte multiplexer mode.

CFP
Indicates coupling facility peer channel.

CIB
Indicates Coupling over Infiniband channel.

CNC
Indicates an ESCON channel path, and that all attached control units and I/O devices support the ESCON Architecture protocol.

CTC
Indicates an ESCON channel path that permits channel-to-channel communications.

CVC
Indicates a channel attached to an ESCON converter and operating in block multiplexer mode. CVC channel paths operate the same as parallel channels operating in block multiplexer mode.

FC
Indicates a native FICON channel path, and that all attached control units and I/O devices support the FICON Architecture protocol.

FCP
Indicates Fibre Channel Protocol channel for SCSI Devices.

ICP
Indicates Internal Coupling facility peer channel.

IQD
Indicates internal queued direct communication (HiperSockets).

OSC
Indicates an OSA channel that operates as an OSA-Express integrated console controller (OSA-ICC) for 3270 support.

OSD
Indicates an OSA channel for QDIO architectures.

OSE
Indicates an OSA channel for non-QDIO architectures.

OSM
Indicates an OSA channel for intra node management network (INMN).

OSN
Indicates an OSA for network control program (NCP) channel.

Channel Path Configuration Search

Select **Channel Path Configuration Search** to search for a channel path using a PCHID number.

PCHID
Select **PCHID** to search for a channel path using a PCHID number. Specify the PCHID number associated with the channel path you want to find. If a channel path does not have a PCHID (for example, channel path types ICP and IQD), you must use the CSS.CHPID option when searching for the channel path. Also, note that channel paths without a PCHID are always displayed at the bottom of the Channel Path Configuration window.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Channel Path Configuration Search

Select **Channel Path Configuration Search** to search for a channel path using a combination of CSS and CHPID numbers.

CSS.CHPID
Specify the CSS number (in the range 0-F) associated with the channel path you want to find. If a channel path is available to multiple channel subsystems and therefore spanned, the CSS value on the Channel Path Configuration window is SPAN. Specify 's' for the CSS number when searching for a spanned channel path. Specify the CHPID number associated with the channel path you want to find.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Channel Subsystem Information

Select **Channel Subsystem Information** to display the logical channel subsystem information for the selected channel path.

The channel subsystem information displayed is associated with keywords on the IOCP CHPID statement. The CHPID statement defines the characteristics of a channel path.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing.

PCHID identifier
Displays the PCHID identifier, if any, for the selected channel path. A PCHID identifier is assigned by the PCHID keyword.

CHPID identifier
Displays the CHPID identifier for the selected channel path. A CHPID identifier is assigned by the PATH keyword.

Channel subsystems
Displays the channel subsystems a channel path is in. The CSS parameter in the PATH keyword assigns channel subsystems to a channel path.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Channel Subsystem Selection

The **Channel Subsystem Selection** window is displayed when a spanned channel path is selected along with an action to display information that must be associated with a single channel subsystem.

The channel path you selected is spanned (that is, it is in multiple channel subsystems). The action you chose requires that a single channel subsystem (CSS) be selected for the channel path before any information is displayed. Select a CSS from the list and click **OK**.

If the selected channel path belongs to a single CSS and is not spanned, this window is not displayed.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing

PCHID identifier
Displays the PCHID identifier, if any, for the selected channel path. A PCHID identifier is assigned by the PCHID keyword

CHPID identifier
Displays the CHPID identifier for the selected channel path. A CHPID identifier is assigned by the PATH keyword

Channel subsystems
Displays the channel subsystems a channel path is in. Select a CSS.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Select a Link Address

The **Select a Link Address** window is displayed when a channel path is selected that has multiple link addresses and an action is chosen to display information for the control units or input/output (I/O) devices attached to the path.

The channel path you selected has multiple control units with different link addresses The channel path is connected to an ESCON or FICON director. The action you chose requires that a single link address be selected for the channel path before any information is displayed. Select a link address from the list and click **OK**.

If the selected channel path does not have multiple link addresses, this window is not displayed.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing

PCHID identifier
Displays the PCHID identifier, if any, for the selected channel path. A PCHID identifier is assigned by the PCHID keyword

Channel subsystem (CSS)
Displays the channel subsystems a channel path is in. The CSS parameter in the PATH keyword assigns channel subsystems to a channel path.

CHPID identifier
Displays the CHPID identifier for the selected channel path. A CHPID identifier is assigned by the PATH keyword

Link address
Displays each link address associated with the selected channel path.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Select Control Unit

The **Select Control Unit** window is displayed so you can select the control unit for which you want to display device information.

The control units listed are all associated with the same composite path (CSS.CHPID.LINK) you selected. Select a control unit from the list and click **OK**.

Control units are defined by IOCP CNTLUNIT statements. The following columns identify information provided by the parameters and keywords of the CNTLUNIT statements. The column headings are the same as the parameters and keywords, unless stated otherwise.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing.

PCHID identifier
Displays the PCHID identifier, if any, for the selected channel path. A PCHID identifier is assigned by the PCHID keyword.

Channel subsystem (CSS)
Displays the channel subsystems a channel path is in. The CSS parameter in the PATH keyword assigns channel subsystems to a channel path.

CHPID identifier
Displays the CHPID identifier for the selected channel path. A CHPID identifier is assigned by the PATH keyword.

Link address
Displays either the only link address associated with the channel path or the link address you selected. A link address is specified by the LINK keyword on the IOCP CNTLUNIT statement.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Control unit table

The control unit table contains a list of control units associated with the selected path (CSS.CHPID.LINK). The column headings are the same as the keywords on the IOCP CNTLUNIT statement. Select a control unit.

CUNUMBR=
The CUNUMBR keyword identifies the control unit number. The control unit number is a unique, arbitrary identifier for the control unit. Control unit numbers are within the hexadecimal range of 0000 to FFFE, and are assigned by the person who edited the statements.

UNIT=
The UNIT keyword identifies the type of control unit. The control unit type is an alphameric identifier, of up to eight characters.

SHARED=
The SHARED keyword indicates the level of concurrency of input/output requests that a parallel channel allows for a control unit. IOCP sets the control unit type (1 or 2) based on the SHARED parameter on the IOCP CNTLUNIT statement. **Y** indicates a type 1 control unit. **N** indicates a type 2 control unit. The SHARED keyword is meaningful only for TYPE=CVC channel paths but IOCP assigns a level of concurrency for all control units. Therefore, a **Y** or **N** is displayed for all channel path types to indicate whether the control unit is type 1 or 2.

PROTOCL=
The PROTOCL keyword indicates the interface protocol used by a control unit when operating with parallel channel paths to which it is attached. The PROTOCL keyword is meaningful only for TYPE=CVC channel paths. A value of **D** specifies the direct-coupled interlock (DC interlock) protocol. A value of **S** specifies the data streaming protocol as a maximum data rate of 3.0 megabytes per second. A value of **S4** specifies the data streaming protocol at a maximum data rate of 4.5 megabytes per second.

UNITADD=
The UNITADD keyword identifies the ranges of addresses of I/O devices recognized by the control unit.

Multiple ranges of addresses are displayed on separate lines under the first line. The other control unit information is the same for each address range, and is not repeated on the additional lines.

CUADD=
The CUADD keyword identifies the logical address of the control unit.

PATH=
The PATH keyword identifies the channel paths to which the control unit is attached. A control unit may be attached to 1 to 8 channel paths.

CHPID Information

Select **CHPID Information** to display information about a channel path for a specific channel subsystem.

If the selected channel path belongs to more than one channel subsystem (CSS), you will need to select a single CSS before the CHPID information is displayed.

The CHPID information displayed is associated with keywords on the IOCP CHPID statement. The CHPID statement defines the characteristics of a channel path.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing.

PCHID identifier
Displays the PCHID identifier, if any, for the selected channel path. A PCHID identifier is assigned by the PCHID keyword.

Channel subsystem (CSS)
Displays the channel subsystem a channel path is in. The CSS parameter in the PATH keyword assigns channel subsystems to a channel path.

CHPID identifier
Displays the CHPID identifier for the selected channel path. A CHPID identifier is assigned by the PATH keyword.

LSYSTEM
Displays the name of the local system if the selected channel path type is CIB. The local system name is assigned by the LSYSTEM keyword on the IOCP ID statement.

Additional functions on this window include:

OK
To return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

CHPID information table

Displays information about the selected channel path.

Shared
Indicates whether the channel path can be configured on by multiple logical partitions at the same time. **Yes** indicates the channel path is shared. **No** indicates it is not shared. The Shared characteristic is set by the SHARED, PARTITION, NOTPART, IOCLUSTER, and PATH keywords.

REC
The REC parameter indicates whether a channel path is reconfigurable between logical partitions. **Yes** indicates the channel path is reconfigurable. **No** indicates it is not reconfigurable. This parameter is set in the PARTITION keyword.

PARTITION= IOCLUSTER=
If the channel path is not shared, the name of the single logical partition it is assigned to is displayed. If the channel path is shared and the IOCLUSTER= keyword was specified, the I/O cluster name is displayed. If the channel path is shared and the IOCLUSTER= keyword was not specified, nothing is displayed.

The following additional information is displayed only for CIB channel path types.

AID=
Displays the adapter identifier (AID) associated with the host channel adapter on which this channel path is defined. An AID is assigned by the AID keyword.

PORT=
Displays the port number on the host channel adapter to which this channel path is defined. A port number is assigned by the PORT keyword.

CSYSTEM=
Displays the name of the system that connects to the selected channel path. A system name is assigned by the LSYSTEM keyword on the IOCP ID statement. The name of the connecting system for this channel path is assigned by the CSYSTEM keyword.

CPATH
Displays the channel subsystem and CHPID identifier (CSS.CHPID) to which the selected channel path is connected. The connecting channel path information is assigned by the CPATH keyword.

Control Unit Information

Select **Control Unit information** to display the control units attached to the selected channel path.

If the selected channel path belongs to more than one channel subsystem (CSS), you will need to select a single CSS before a list of control units is displayed. Also, if the channel path uses multiple link addresses on a Director, you will need to select a single link address. Then all the control units assigned to the composite path CSS.CHPID.LINK are displayed.

Control units are defined by IOCP CNTLUNIT statements. The following columns identify information provided by the parameters and keywords of the CNTLUNIT statements. The column headings are the same as the parameters and keywords, unless stated otherwise.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing.

PCHID identifier
Displays the PCHID identifier, if any, for the selected channel path. A PCHID identifier is assigned by the PCHID keyword.

Channel subsystem (CSS)
Displays the channel subsystems a channel path is in. The CSS parameter in the PATH keyword assigns channel subsystems to a channel path.

CHPID identifier
Displays the CHPID identifier for the selected channel path. A CHPID identifier is assigned by the PATH keyword.

Link address
Displays either the only link address associated with the channel path or the link address you selected. A link address is specified by the LINK keyword on the IOCP CNTLUNIT statement.

Additional functions on this window include:

OK
To return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Control unit table

The control unit table contains a list of control units associated with the selected path (CSS.CHPID.LINK). The column headings are the same as the keywords on the IOCP CNTLUNIT statement.

CUNUMBR=
The CUNUMBR keyword identifies the control unit number. The control unit number is a unique, arbitrary identifier for the control unit. Control unit numbers are within the hexadecimal range of 0000 to FFFE, and are assigned by the person who edited the statements.

UNIT=
The UNIT keyword identifies the type of control unit. The control unit type is an alphameric identifier, of up to eight characters.

SHARED=
The SHARED keyword indicates the level of concurrency of input/output requests that a parallel channel allows for a control unit. IOCP sets the control unit type (1 or 2) based on the SHARED parameter on the IOCP CNTLUNIT statement. **Y** indicates a type 1 control unit. **N** indicates a type 2 control unit. The SHARED keyword is meaningful only for TYPE=CVC channel paths but IOCP assigns a level of concurrency for all control units. Therefore, a **Y** or **N** is displayed for all channel path types to indicate whether the control unit is type 1 or 2.

PROTOCL=
The PROTOCL keyword indicates the interface protocol used by a control unit when operating with parallel channel paths to which it is attached. The PROTOCL keyword is meaningful only for TYPE=CVC channel paths. A value of **D** specifies the direct-coupled interlock (DC interlock) protocol. A value of **S** specifies the data streaming protocol as a maximum data rate of 3.0 megabytes per second. A value of **S4** specifies the data streaming protocol at a maximum data rate of 4.5 megabytes per second.

UNITADD=
The UNITADD keyword identifies the ranges of addresses of I/O devices recognized by the control unit.

Multiple ranges of addresses are displayed on separate lines under the first line. The other control unit information is the same for each address range, and is not repeated on the additional lines.

CUADD=
The CUADD keyword identifies the logical address of the control unit.

PATH=
The PATH keyword identifies the channel paths to which the control unit is attached. A control unit may be attached to 1 to 8 channel paths.

Device Information

Select **Device Information** to display the information specified for the parameters and keywords of IODEVICE statements.

If the selected channel path belongs to more than one channel subsystem (CSS), you will need to select a single CSS before a list of control units is displayed. Also, if the channel path uses multiple link addresses on a Director, you will need to select a single link address. Then all the control units assigned to the composite path CSS.CHPID.LINK are displayed. If the composite path has multiple control units, you will need to select a single control unit. Then all the devices associated with the selected control unit and path are displayed.

Input/output devices are defined by IOCP IODEVICE statements. The following columns identify information provided by the parameters and keywords of the IODEVICE statements. The column headings are the same as the parameters and keywords, unless stated otherwise.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing.

PCHID identifier
Displays the PCHID identifier, if any, for the selected channel path. A PCHID identifier is assigned by the PCHID keyword.

Channel subsystem (CSS)
Displays the channel subsystems a channel path is in. The CSS parameter in the PATH keyword assigns channel subsystems to a channel path.

CHPID identifier
Displays the CHPID identifier for the selected channel path. A CHPID identifier is assigned by the PATH keyword.

Additional functions on this window include:

OK
To return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Device table

The device table contains a list of devices assigned to the selected control unit. The column headings are the same as the keywords on the IOCP IODEVICE statement.

UNITADD=
The UNITADD keyword identifies the physical unit address assigned to the I/O device. A physical unit address identifies an I/O device to the control units to which it is attached.

ADDRESS=
The ADDRESS keyword identifies the device number.

SCHSET=
The SCHSET keyword identifies the subchannel set in the selected CSS to which this device belongs.

UNIT=
The UNIT keyword identifies the type of I/O device. The device type is an alphameric identifier, of up to eight characters.

MODEL=
The MODEL keyword identifies the model number of the I/O device. The model number is an alphameric identifier, of up to four characters.

STADET=
The STADET keyword indicates whether the Status Verification Facility is enabled. A value of **Y** indicates the Status Verification Facility is enabled. A value of **N** indicates the Status Verification Facility is not enabled.

TIMEOUT=
The TIMEOUT keyword indicates whether the I/O interface time-out function is active. A value of **Y** indicates the I/O interface time-out function is active. A value of **N** indicates the I/O interface time-out function is not active. The TIMEOUT keyword is meaningful only for TYPE-CVC channel paths. Devices assigned to TYPE=CBY channel paths always have the time-out function active. For all other channel path types, the timeout function is not active.

Image Candidate List

Select **Image Candidate List** to display the logical partitions for a specific channel subsystem that can access the channel path.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing.

PCHID identifier
Displays the PCID identifier, if any, for the selected channel path. A PCHID identifier is assigned by the PCHID keyword.

Channel subsystem (CSS)
Displays the channel subsystems a channel path is in. The CSS parameter in the PATH keyword assigns channel subsystems to a channel path.

CHPID identifier
Displays the CHPID identifier for the selected channel path. A CHPID identifier is assigned by the PATH keyword.

Image candidate list table

MIF image ID
The MIF image ID within the CSS that is associated with the logical partition.

Partition name
The name of a logical partition in the image candidate list for the selected channel path and CSS.

Additional functions on this window include:

OK
To return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

Image Access List

Select **Image Access List** to display the logical partitions for a specific channel subsystem that have the channel path configured online at partition activation following initial power-on reset (POR) of the IOCDS.

After the initial POR of the IOCDS, PR/SM LPAR retains which logical partitions will have the channel path configured online at partition activation following subsequent PORs with the same IOCDS.

The image access list displayed is associated with keywords PARTITION, NOTPART, SHARED, and PATH on the IOCP CHPID statement.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing.

PCHID identifier
Displays the PCHID identifier, if any, for the selected channel path. A PCHID identifier is assigned by the PCHID keyword.

Channel subsystem (CSS)
Displays the channel subsystems a channel path is in.

CHPID identifier
Displays the CHPID identifier for the selected channel path. A CHPID identifier is assigned by the PATH keyword.

Image access list table

MIF image ID
The MIF image ID within the CSS that is associated with the logical partition. For a null image access list, this field is left blank.

Partition name
The name of a logical partition in the image access list for the selected channel path and CSS. If the channel path has a null image access list, a zero is displayed. A null image access list indicates that no logical partitions in the CSS will access the channel path following partition activation for the initial POR of the IOCDS.

Additional functions on this window include:

OK
To return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

Function ID Configuration

Use the **Function ID Configuration** window to select a channel configuration data set of information you want to view. The table lists the FIDs and assigned PCHID that exist in the selected IOCDS.

The function configuration table display:

FID
Displays the Function ID for the selected configuration data set

TYPE
Displays the function type the card is defined as

PCHID
Displays a four-digit physical channel identifier (PCHID) for the selected configuration data set.

PORT
Displays the port assignment for a specific Function ID

VF
Displays the virtual function for the selected configuration data set

UUID
Displays the unique user-defined ID for the configuration data set

Access Partition Name
Displays the partition name the configuration data set

PNETID
Displays the physical network identifier configuration data set.

The icons perform the following actions for the selected configuration data set:

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want.

Clear All Filters
Click **Clear All Filters** to return to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Additional functions on this window include:

Close
To close the current window and return to the previous window, click **Close**.

Help
To display help for the current window, click **Help**.

Image Candidate List

Select **Image Candidate List** to display the logical partitions for a specific channel subsystem that have the FID configured online at partition activation following initial power-on reset (POR) of the IOCDS.

After the initial POR of the IOCDS, PR/SM LPAR retains which logical partitions will have the FID configured online at partition activation following subsequent PORs with the same IOCDS.

The image candidate list displayed is associated with keywords PARTITION, NOTPART, SHARED, and PATH on the IOCP CHPID statement.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing.

PCHID
Displays the PCHID identifier, if any, for the selected FID. A PCHID identifier is assigned by the PCHID keyword.

FID
Displays the FID identifier for the selected channel. A FID identifier is assigned by the PATH keyword.

Partition Name
Displays the Partition Name for the FID.

Additional functions on this window include:

Close
To close the current window and return to the previous window, click **Close**.

Help
To display help for the current window, click **Help**.

Partition Images Configured

Select **Partition Images Configured** to display the MIF image ID numbers and names of the logical partitions defined in the selected input/output configuration data set (IOCDS).

You can sort the list of logical partitions by partition name or by CSS and MIF image ID numbers.

Configuration data set
Displays the identifier of the configuration data set that you selected and are viewing.

Partition images configuration table

The partition images configuration table displays all of the logical partitions defined in the selected IOCDS. All the following logical partition information is specified with the PARTITION keyword on the RESOURCE statement.

CSS
The CSS parameter indicates the channel subsystem a logical partition is in.

MIF Image ID
The MIF image ID within the CSS that is associated with the logical partition.

Partition Name
The name of the logical partition.

Dynamic Information

Select **Dynamic Information** to check and compare an input/output configuration data set (IOCDS) token and the current channel subsystem hardware system area (HSA) token. If the selected IOCDS does not have a token, it does not contain any dynamic information and the Dynamic Information view cannot be selected.

Configuration data set shows the identifier of the IOCDS you selected on the previous window. Its token displays in the **Data set token** field. An IOCDS has a token if it was created using an operating system feature that supports dynamically changing the input/output (I/O) definition defined by the IOCDS.

Hardware system area token shows current HSA token, if any. The HSA token is only displayed if the system has been power-on reset using an IOCDS that had a token in it and the power-on reset enabled dynamic I/O configuration.

Configuration data set
Displays the identifier of the configuration data set.

Data set token
Displays the IOCDS token.

Hardware system area token

Displays the token most recently saved in the hardware system area (HSA). A token is saved in the HSA when:

- A power-on reset is performed using an IOCDS that contained a token and the power-on reset enabled dynamic I/O configuration.
- An operating system feature that supports dynamically changing the I/O definition is used to alter the HSA.

If the most recent power-on reset did not enable dynamic I/O configuration changes, this field is blank.

When the HSA token and the data set token match, and the data set is active, the operating system feature can be used to dynamically change the I/O definition.

Data set maximum number of devices
Displays the maximum number of devices allowed for each channel subsystem (CSS) and each subchannel set. This is defined by IOCP with the MAXDEV keyword on the RESOURCE statement.

Hardware system area maximum number of devices
Displays the maximum number of devices allowed for each channel subsystem (CSS) and each subchannel set within the HSA. These maximums are established during power-on reset and cannot be changed dynamically.

If the most recent power-on reset did not enable dynamic I/O configuration changes, this field is blank.

Additional functions on this window include:

OK
To return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

Supported I/O Mask

Select **Supported I/O Mask** to display and compare the supported I/O masks in the selected IOCDS and supported by your CPC.

The supported I/O mask contains hexadecimal values that identify the processor functions or channel path types defined in the IOCDS or supported by your CPC. If the IOCDS contains a value not in the Machine Supported I/O mask, then the Unsupported mask items display shows which items are not supported by the system. The system cannot power-on reset with the selected IOCDS.

See "CPC activation and Power-on Reset Error" in the *Input/Output Configuration Program User's Guide* for a description of the supported functions and channel path types.

IOCDS supported I/O mask
The supported I/O mask in the IOCDS indicating the functions and channel path types contained in the IOCDS.

Machine supported I/O mask
The supported I/O mask for the machine indicating all the functions and channel path types supported by the machine.

Unsupported mark items
The specific items in the IOCDS that are not supported by the machine. This line is displayed only when unsupported items are present. The IOCDS cannot be used to power-on reset the machine.

Additional functions on this window include:

OK
To return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

Save Data Files on Hardware Management Console

Use this window to copy the IOCDS data files from the Support Element console to the Hardware Management Console's hard drive. The fully qualified path name for the data files must be specified at the Target path name entry field.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Restore Data Files on Hardware Management Console

Use this window to copy the IOCDS data files from the Hardware Management Console's hard drive to the Support Element's hard drive. The fully qualified path name for the data files must be specified at the Target path name entry field.

Additional functions on this window include:

OK
To perform the selected action, click **OK**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Installation Complete Report

Accessing the Installation Complete Report task

Note: You cannot perform this task remotely.

This task is used by support system personnel to report installation information. This information is used to assess the success of the installation and make improvements in the installation processes. The information can be transmitted directly to the support system from the Hardware Management Console or copied to removable media.

The following types of installations should be reported:

- New install
- MES (Miscellaneous Equipment Specification)
- Reinstall
- Patch, Ucode, LIC
- Refresh, PTF
- Discontinue.

To provide an installation complete report:

1. Open the **Installation Complete Report** task. The Installation Complete Report window is displayed.
2. Provide the appropriate information to complete the report.
3. Click **Continue** to proceed to the next window to provide more information or proceed with the process of transmitting the report to the support system.

Installation Complete Report (installation activities)

Use this window to fill in and send product support a report about installation activities for a customer's Support Element. You should report any of the following installation activities:

- Installing new machines.
- Upgrading previously installed machines (MES).
- Reinstalling previously installed machines.
- Changing licensed internal code of machines.

- Upgrading corrective service levels of machine control programs (refresh or PTF).
- Removing previously installed machines (Discontinue).

An installation complete report should take only a few minutes to complete. The information in the report helps product support to maintain field inventory databases and to identify, resolve, and prevent defects.

Team Leader Name
Specify your name, or the name of the person to contact about the installation and the information in this report.

Telephone number
Specify your telephone number, or the telephone number of the person to contact about the installation and the information in this report.

Specify the three-digit area code in the leftmost field, then use the middle and rightmost fields to specify the seven-digit local number.

Activity Group
This section identifies the types of activities performed during the installation. You must select at least one of the following types of activity, but you can select more than one or all of the types of activities.

New install
Indicates the installation activities included installing one or more new machines.

MES
Indicates the installation activities included upgrading one or more previously installed machines.

Re-install
Indicates the installation activities included installing again one or more previously installed machines.

Patch, Ucode, LIC
Indicates the installation activities included changing the licensed internal code for one or more machines.

Refresh, PTF
Indicates the installation activities included upgrading the corrective service level of the control program for one or more machines.

Discontinue
Indicates the installation activities included removing one or more previously installed machines.

Continue
When you are finished providing the information requested on the window, click **Continue**. This displays the next window in the current report.

Cancel
To discard the current report and close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Installation Complete Report (date and time checkpoints)

Use this window to report the date and time when installation checkpoints were completed, and to indicate whether the installation was defect-free.

Machine arrival date/time
Use these fields to specify the date and time the hardware was delivered to the installation site. The format of the date is: **mm/dd/yy** or you can click the calendar icon and make a selection. The format of the time is: **hh:mm:ss AM** (or **PM**), or click the clock icon and specify the time in the fields provided.

Install start date/time
Use these fields to specify the date and time the first installation activity was started. The format of the date is: **mm/dd/yy** or you can click the calendar icon and make a selection. The format of the time is: **hh:mm:ss AM** (or **PM**), or click the clock icon and specify the time in the fields provided.

Mechanical complete date/time
Use these fields to specify the date and time the final hardware installation activity was completed. The format of the date is: **mm/dd/yy** or you can click the calendar icon and make a selection. The format of the time is: **hh:mm:ss AM** (or **PM**), or click the clock icon and specify the time in the fields provided.

Solution software complete date/time
Use these fields to specify the date and time the final software installation activity was completed. The format of the date is: **mm/dd/yy** or you can click the calendar icon and make a selection. The format of the time is: **hh:mm:ss AM** (or **PM**), or click the clock icon and specify the time in the fields provided.

Install complete date/time
Use these fields to specify the date and time the final installation activity was completed. The format of the date is: **mm/dd/yy** or you can click the calendar icon and make a selection. The format of the time is: **hh:mm:ss AM** (or **PM**), or click the clock icon and specify the time in the fields provided.

Total idle time
Specify the total amount of time spent not performing any installation activities between starting the first installation activity and completing the final installation activity.

Then use the **Explain idle time or missed commitment** field to specify an explanation of the reasons for the idle time.

Was commitment to customer met?
To indicate **the customer's** expectations for the installation were met, select **Yes**.

Otherwise, if **the customer's** expectations for the installation were not met, select **No**. Then use the **Explain idle time or missed commitment** field to specify an explanation of the reasons the commitment was not met.

Explain idle time or missed commitment
Specify an explanation of the reasons for any idle time, or why the commitment to the customer was not met. That is, specify an explanation when:

- You specified any non-zero amount of time in the **Total idle time** field, or
- You selected **No** to answer **Was commitment to customer met?**

Were problems encountered?
To indicate one or more problems occurred during the installation, select **Yes**. Otherwise, select **No**.

A problem is any event that:

- Prevents the completion of the installation.
- Delays the completion of the installation.
- Requires performing activities during the installation that would not be performed if the event had not occurred.

  Example: Removing and replacing a defective part.

Continue
When you are finished providing the information requested on the window, click **Continue**.

If you selected **No** to answer **Were problems encountered?**, then the report is complete. Clicking **Continue** starts the process for transmitting the report to the support system.

Otherwise, if you answered **Yes** to indicate one or more problems occurred, then you must provide more information about each problem. Clicking **Continue** displays additional windows for reporting problem information.

Cancel
To discard the information on this window, and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Installation Complete Report (additional information for a problem)

On a previous window, you indicated problems were encountered during the installation. Use this window to provide more information about one of the problems.

A problem is any event that:

- Prevents the completion of the installation.
- Delays the completion of the installation.
- Requires performing activities during the installation that would not be performed if the event had not occurred.

  Example: Removing and replacing a defective part.

System lost time
Specify the amount of time the system was not available because of the problem.

Problem resolution time
Specify the amount of time required to diagnose and correct the problem.

Part procurement time
Specify the amount of time between requesting and receiving parts required to correct the problem.

Defect Summary
This section describes the cause of the problem, and describes how the problem was solved.

For each field, you can select the term that best describes the information it requests by clicking the scroll arrow for a list of choices or you can specify a new entry.

Component
Select or specify the term that best describes the specific unit of hardware, software, or documentation that caused the problem.

Action
Select or specify the term that best describes how the problem with the component was solved.

Source
Select or specify the term that best describes the general unit of hardware, software, or documentation that contained the component that caused the problem.

Defect
Select or specify the term that best describes the problem with the component.

Parts not Recorded by Repair and Verify
If you removed and replaced a part while diagnosing or correcting the problem, but were not instructed to do so by an online service procedure, then use this section to describe the part you removed and the part that replaced it.

Reference code
Specify the reference code, if any, for the problem.

Part number
Specify the Custom Card Identification Number (CCIN) of the removed part.

Serial number
Specify the serial number of the removed part.

Location
Specify the part location from which the part was removed.

Note: If the removed part is identified by two part locations, specify the first location in this field, then specify the second location in the **To location** field. For example, cables are identified by two part locations. Each part location identifies where one end of the cable is connected.

To location
If the removed part is identified by two part locations, specify the second part location from which the part was removed. Specify the first location in the **Location** field.

Note: For example, cables are identified by two part locations. Each part location identifies where one end of the cable is connected.

New part number
If a different part was installed to replace the removed part, specify the Custom Card Identification Number (CCIN) of the replacement part.

New serial number
If a different part was installed to replace the removed part, specify the serial number of the replacement part.

BOM number
If the replacement part was ordered new, specify the number of its Bill of Materials (BOM).

Patch or MCL fixes
If you installed and activated an internal code fix while correcting the problem, use this section to specify the Engineering Change (EC) number of the internal code fix in the **Patch number** field.

Comments about the defect
Specify any additional information that describes the problem or its solution.

Continue
When you are finished providing the information requested on the window, click **Continue**. A message displays for you to use to indicate whether there are additional problems to report.

Cancel
To discard all problem information on the window and in the current report, and to return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Part Location

Part Location identifies the location of a part in a frame.

Parts can be located in the power module section or card section within a Central Processor Complex (CPC) or an optional expansion cage.

Part locations are identified by up to twelve characters. Some parts, like cables, are identified by up to twelve characters for the location of each end, with the two locations separated by a dash.

The first character of a twelve character location identifies the frame location.

A
Identifies the rightmost frame in the machine.

Z, Y, X, W, or V
Identifies frames attached to the left of frame A.

Note: The identifiers used for additional frames are determined by the machine model.

The next three characters identify the location of the CPC or expansion cage within the frame.

01A
Indicates the location is the bottom of the frame.

18A
Indicates the location is the top of the frame.

The remaining four to eight characters identify the type of part, and indicate where the part is located within the CPC or expansion cage.

- For the following parts in the card section, 'nn' identifies the card socket where the part is located:

D1nn
Coupling facility channel link card

D2nn
Coupling facility channel link card

LGnn
Logic card

Example: A logic card in card socket 26 of the CPC or expansion cage at the bottom of frame Y is identified by part location:

Y01ALG26

- For the following parts in the power module section, 'nn' is a number that distinguishes a module from other modules of the same type:

AFnn
AC front end card (power module)

BUnn
Battery backup module

ELnn
Energy limiting module

PSnn
Power supply, AC/DC modules

UPnn
Unit panel (central processor complex)

Example: The second of two energy limiting modules in the top CPC in frame A is identified by part location:

A18AEL02

Interrupt

Accessing the Interrupt task

An *interrupt* is a processor operation you can use to present an external interruption to a processor. If you have experience using other systems, you may have used an IRPT command or an Irpt key to interrupt a processor.

Follow your local procedures for determining when to interrupt a processor. You can use the Support Element workplace to interrupt any eligible processor. Eligible processors include:

- Physical processors that support the image of a central processor complex (CPC).
- Logical processors that support the images of logical partitions activated in operating modes other than coupling facility mode.

To interrupt a processor:

1. Open the **Interrupt** task.

   This immediately performs the operation; an interrupt request is generated for the processor.

Load

Accessing the Load task

Notes:

- A load resets a system or logical partition, to prepare it for loading an operating system, and then loads the operating system. You can have up to four Load types: **ECKD**, **SCSI**, **NVMe**, **Tape**.

- For daily or routine loading of images, it is recommended that you customize activation profiles to specify how you want to load images, and then use a profile with the **Activate** task to perform all the operations necessary to make an image operational, including loading it with a control program.
- The **Load** task is considered a disruptive task. If the object is locked, you must unlock it before continuing.

Load (except coupling facility and SSC images) causes a program to be read from a designated device and initiates execution of that program. On the Support Element workplace, **images** support operating systems, so images are your targets for loads. An image represents a logical partition, while the CPC is activated.

Follow your local error recovery procedures for determining when to perform a load.

To perform a load:

1. Open the **Load** task. The Load window is displayed with the information that was last used when the CPC image was loaded
2. Review the information in the window to verify that the object you will load is the correct one.

   If the information is correct, click **OK**. The Load Task Confirmation window is displayed. If you click **Yes** to proceed, then the Disruptive Task Confirmation window is displayed. Review the confirmation text to decide whether or not to proceed with the task.
3. To continue with the load, click **Yes**. The Load Progress window is displayed indicating the progress of the load and the outcome.
4. Click **OK** to close the window when the load completes successfully. Otherwise, if the load does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

Load

Use this window to provide or change information used to load the selected images with a control program. Use this window while “Loading an image during a recovery procedure” on page 641.

Note: For daily or routine loading of images, It is recommended that you customize activation profiles to specify how you want to load images and then use a profile with the **Activate** task to perform all the operations necessary to make an image operational, including loading it with a control program.

Note: Other products and documentation may refer to this operation as an *initial program load (IPL)*.

Select the image to display load information you want to view.

1. Review or change the information displayed on the window. It will be used to load the selected image with a control program.
2. Click **OK** to request a load using the displayed information.

Loading an image during a recovery procedure

You can use a Hardware Management Console to load an image. You can try to load any image at any time, but this task is intended for use during recovery procedures.

Note: For daily or routine loading of images, the following alternative is recommended:

1. Use the **Activation Profiles** task to customize and store load information in activation profiles for Central Processor Complexes (CPCs) and their images.
2. Use the **Activate** task and a profile to perform all the operations necessary to make a CPC or image operational, including loading it with a control program.

Use this window to customize information that controls loading a control program :

CPC
Displays the name of the central processor complex (CPC) that supports the selected image.

Image
Depending on your model and machine type, you may have only logically partitioned (LPAR) mode or both LPAR mode and General mode. If the CPC is operating in LPAR mode, this field displays the name of the logical partition that supports the selected image. The logical partition is the target of the load.

An **image** is a set of CPC resources capable of running a control program or operating system. One or more images are created during a power-on reset of a CPC. When a power-on reset puts the CPC in LPAR mode, each logical partition is an image. When a power-on reset puts the CPC in a General mode, the CPC has a single image.

Device type
Select the type of device to perform a load for the logical partition. You would use the SCSI or NVMe option to do a standalone dump to a SCSI device or NVMe adapter.

ECKD
To perform an IPL on the logical partition from ECKD DASD load type, click **ECKD**. Optionally, select **Load a dump program** load type to the clear main storage on the logical partition before loading.

SCSI
To perform an IPL on the logical partition from SCSI load type, click **SCSI**.

NVMe
To perform an IPL on the logical partition from NVMe load type, click **NVMe**.

Tape
To perform an IPL on the logical partition from Tape load type, click **Tape**. Optionally, select **Load a dump program** load type to clear main storage on the logical partition before loading .

IPL type:
Select the type of IPL for the selected **ECKD** device type to perform for the logical partition.

Channel Command Word (CCW)
To perform the load on CCW IPL, click **Channel Command Word (CCW)**.

List-directed
To perform the load on a list-directed IPL, click **List-directed**.

If the selected load type is **SCSI**, **NVMe**, or **Tape**, this field is unavailable.

Load type:
Select the type of load to perform for the logical partition. Optionally, for **ECKD** or **Tape** select clear main the memory before loading. You would use the **ECKD** or **Tape** option to do a standalone dump and select the **Load a dump program** option.

Load an OS
To perform an operating system load type on the logical partition, click **Load an OS**.

Load a dump program
To perform a dump program load type on the logical partition, click **Load a dump program**.

Validation:

Enable Secure Boot
To verify the signature of the load program and distributor's signature match, select **Enable Secure Boot**.

Certificates
The Certificates table displays the imported certificates assigned to the partitions.

If the selected load type is **Tape**, this field is unavailable.

Options:

Store status
The store status function stores the current values of the processing unit timer, the clock comparator, the program status word, and the contents of the processor registers in their assigned absolute storage locations.

If the **Load a dump program** type is selected, click the check box to change the setting.

- A check mark indicates performing the store status function before the load.
- An empty check box indicates not performing the store status function before the load.

Clear the main memory before loading
Select this to clear main memory storage on the logical partition before a load. Clearing partitions with larger amount of main memory storage may take longer.

Note: Available when the **Load an OS** type is selected for the Load type.

Load address:

Enter the address of the input/output (I/O) device that provides access to the control program to load. For a SCSI load or NVMe load, this field has the device number of the device (for example, fibre channel adapter) that is used to perform the SCSI or NVMe load. This should contain four hexadecimal digits for NVMe load or five hexadecimal digits for SCSI load.

A load address is required.

The source of the control program must be an I/O device in the I/O configuration that is active when this profile is activated. The I/O device can store the control program or can be used to read the control program from a data storage medium.

Note: This field is applicable only when **Use dynamically changed address** check box is empty. Otherwise, if the check box displays a check mark, this field is unavailable.

Use dynamically changed address

To indicate whether the load address is dynamically determined by changes to the channel subsystem Input/Output definition (I/O), select **Use dynamically changed address**.

If this is selected, the load address is dynamically determined. Otherwise, this profile sets the load address. See the **Load address** field for the address set by this profile.

Specify the address in the **Load address** field.

Load parameter:

Specify the optional information, if any, to use to further control how the control program is loaded during activation. Valid characters for a load parameter are:

- At (@)
- Pound (#)
- Dollar ($)
- Blank character
- Period (.)
- Decimal digits 0 through 9
- Capital letters A through Z.

Some control programs support the use of a load parameter to provide additional control over the performance or outcome of a load. Check the configuration programming and reference documentation for the control program to determine the load parameters that are available and their effects on a load.

Note: This field is applicable only when **Use dynamically changed parameter** is **not** selected. Otherwise, this field is unavailable.

Use dynamically changed parameter

To indicate whether the load parameter is dynamically determined by changes to the channel subsystem Input/Output (I/O) definition, select **Use dynamically changed parameter**

If this is selected, the load parameter is dynamically determined. Otherwise, this profile sets the load parameter. Enter the parameter for this profile in the **Load parameter** field.

Time-out value:

Specify the amount of time to allow for the completion of the load.

The time-out value can be from 60 to 600 seconds. If the load operation cannot be completed within the specified time, the operation is canceled.

If the selected load type is **SCSI** or **NVMe**, this field is unavailable.

Boot record location:

The boot record location (C,H,R format) parameters can be specified from the volume label or be specified.

- Select **use volume label** to specify the boot record label from the volume label
- Select to specify the C,H,R format. The Cylinder number is a 4-byte value ranging from '0x00000000' to '0x0FFFFFFF'. The Head number is a 1-byte value ranging from '0x00' to '0x0F'. The Record number is a 1-byte value ranging from '0x01' to '0xFF'.

If the selected load type is **SCSI**, **NVMe**, or **Tape**, this field is unavailable.

Worldwide port name:

Specify the Worldwide Port Number identifying the Fibre Channel port of the SCSI target device (according to the FCP/SCSI-3 specifications). This is a 64-bit binary number designating the port name, represented by 16 hexadecimal digits. This is required for SCSI load or SCSI dump.

If the selected load type is **ECKD**, **NVMe** , or **Tape**, this field is unavailable.

Logical unit number:

Specify the number of the logical unit as defined by FCP (according to the FCP/SCSI-3 specifications). This is the 64-bit binary number designating the unit number of the FCP I/O device, represented by 16 hexadecimal digits. This field is required for SCSI load or SCSI dump.

If the selected load type is **ECKD**, **NVMe** , or **Tape**, this field is unavailable.

Boot program selector:

This field identifies the program to load from the FCP-load device and contains a decimal value in the range from 0 to 30. This parameter provides the possibility of having up to 31 different boot configurations on a single disk device. This field should be set to 0 for optical media SCSI devices.

If the selected load type is **Tape**, this field is unavailable.

Boot record logical block address:

Specify the load block address if your file system supports dual-boot or booting from one of the multiple partitions. If no block address is specified, the logical-block address of the boot record is assumed to be zero. This feature could be used to IPL using a second or backup boot record, in case the original one is corrupted or overwritten by accident.

If the selected load type is **ECKD** or **Tape**, this field is unavailable.

Operating system load parameters:

Specify a variable number of characters to be used by the program that is loaded. This information will be given to the IPLed operating system and will be ignored by the machine loader. The IPLed operating system (or standalone dump program) has to support this feature. Any line breaks you enter are transformed into spaces before being saved.

If the selected load type is **Tape**, this field is unavailable.

Additional functions on this window include:

OK

To load the selected image, click **OK**.

Reset
To erase the information you typed and re-display the information most recently used to load the selected image, click **Reset**.

Cancel
To exit this window and return to the Hardware Management Console workplace without performing the load, click **Cancel**.

Help
To display help for the current window, click **Help**.

Load Processor from File

Load Processor From File

Use this window to load the selected central processor (CP) from a file. The file must be stored on a CD or DVD. Be prepared to insert the CD or DVD in the support element's DVD drive.

To load the CP from a file stored on a CD or DVD:

1. Insert the CD or DVD into the support element's DVD drive.
2. Type the file name and extension in the *Filename* field.
3. Click **OK** to begin loading the file.
4. Wait until a message indicates loading the file has completed.
5. Click **OK** to close the message.

Filename
Type the file name and extension of the file you want to load.

A file name and extension can have up to 12 characters.

- A file name can have one to eight characters.
- A file extension can have zero to three characters.
- The file name and extension must be separated by a period.

The file must be stored on a CD or DVD. Be prepared to insert the CD or DVD in the support element's DVD drive.

Loading the file copies its contents to the selected central processor's main storage, beginning at storage address 0.

Location address
Type the storage address at which you want to begin loading the selected central processor (CP).

Loading the CP from a file loads the contents of the file you specify to the CP's main storage, beginning at the address you specify.

OK
To begin loading the CP with the file, click **OK**.

Reset
To clear the *Filename* entry field (the current entry, if any, will be discarded), click **Reset**.

Cancel
To close the window without loading the CP, click **Cancel**.

Help
To display help for the current window, click **Help**.

Load from Removable Media or Server

Accessing the Load from Removable Media or Server task

This task loads system software or utility programs from removable media or from an FTP server.

Note: The installation of some software, such as certain levels of z/VM, requires you to not remove the media from the Hardware Management Console's drive until directed. For more information, see the installation instructions that come with your software.

To load the software:

1. Open the **Load from Removable Media or Server** task.

   The Load from Removable Media or Server window displays.
2. Select the source of the software:
   - Local removable media device
   - FTP Server

     If you are loading from an FTP server, you need to:

     – Enter the FTP host name.
     – Enter your user name.
     – Enter your password.
     – Select the FTP protocol.
3. Choose the location of the software program by specifying the relative or absolute file path on the **File path** field, if necessary.
4. Click **OK**.
5. Proceed with the "Select Software to Install" on page 647 window by selecting the **.ins** file and performing the load.
   - If you used Single Object Operations to access this Support Element from a Hardware Management Console, and the source is in the root directory of the CD/DVD-ROM, select **Hardware Management Console removable media device**, and leave the File location blank.
   - **Relative Path:** If you used Single Object Operations to access this Support Element from a Hardware Management Console, and the source is in the LINUX subdirectory, you can select **Hardware Management Console removable media device** and enter `LINUX` (or `LINUX/`) in the File location. (Note that the path name is case-sensitive.)

   The File location field works the same way whether the source you choose is the Hardware Management Console's removable media device or the FTP server.
6. After you complete the current window and select the file or program you want to load, click **OK** to continue with this task. A load in-progress window is displayed showing the duration and elapsed times.
7. Click **OK** to close the window when the task completes successfully.

Load from Removable Media or Server

This task loads system software or utility programs from removable media, or from an FTP protocol. You can specify only one software source.

Note: For any of the sources of the software that you select, you must prepare the **.ins** file and the actual software or programs to load on the source using the "Select Software to Install" on page 647 instructions.

Local removable media device
To retrieve operating system software or utility programs from the local removable media device use, select **Local removable media device**.

If you use **CD/DVD-ROM** as the source, the ISO image must be burned using the ISO1996 file system format.

FTP Server
To retrieve operating system software or utility programs from an FTP source, select **FTP Server**.

When want to use an **FTP server** as the source, make sure the Support Element has access to the target FTP server using one of these protocols: FTP (File Transfer Protocol), FTPS (FTP Secure), or SFTP (SSH File Transfer Protocol).

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

OK
To continue to load from removable media or server, click **OK**.

Cancel
To close the window and exit this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Select Software to Install

This Load from Removable Media to Server - Select Software to Install window allows you to load software or utility programs from the Hardware Management Console's removable media, from local removable media, or from an FTP server.

Select the software or utility program to load. Use your cursor movement keys or your mouse to highlight the selection, then click **OK** to proceed. Only one selection is allowed at a time.

After you specify the system software or utility program to load, all files within that package are loaded into the target and started. The **.ins** files represent packages of software or programs that can be loaded. They have a file extension of **ins.** and are in the form:

*Description line
/relative path/filename1.extension < space > < address of where to load >
/relative path/filename2.extension < space > < address of where to load >
/relative path/filename3.extension < space > < address of where to load >
.
.
.
/relative path/filenameN.extension < space > < address of where to load >

Where **path** is relative to the location of the **ins** file.

For example, **Sample1.ins** could contain:

** SuperUtilities Package Version 12.34*
/directory1/file1.txt 0x00000000
/directory2/file2.txt 0x00100000

All addresses start with "0x", followed by an 8 character hexadecimal address of where to start to load the file in memory.

An asterisk (*) in the first line of the file starts a comment line and is used to supply a one-line description of the file used on this window and on the confirmation window. The remainder of the file is a list of which files on the source (relative to where the load control file is located) and the addresses of where to load the data.

Generally, data files are a multiple of 4 bytes. If a file is only 2 bytes long and contains 0x1234, then 4 bytes are loaded into memory as 0x12340000. The highest address allowed is 0x7FFFFFFF. **Load from removable media device or FTP server** is intended for loading a software or utility installation program, not for normal IPLs.

Software table
Displays a list of the operating system software or utility programs that you want to retrieve.

OK
To proceed with loading the selected software or utility program to removable media or to an FTP server, click **OK**.

Cancel
To return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Logical Processor Add

Accessing the Logical Processor Add task

You can use the Support Element workplace to start the task that allows you to select logical processor definitions to be changed dynamically on the system, in the image profile, or both. Dynamic changes will take effect without performing a reactivation of the logical partition.

The initial control settings of each logical partition are established by the activation profiles used to activate them. See the following topics for more information about customizing activation profiles for establishing initial control settings:

- Assigning initial logical or reserved processors
- Setting workload manager (WLM) controls

To dynamically add one or more logical processors to a logical processor:

1. Open the **Logical Processor Add** task.

   The Logical Processor Add window displays.
2. Based on the current logical partition configuration, change the logical processor definitions for the partition:
   - Increase the initial values, reserved values, or both for installed logical processor types.
   - Add a reserved value and set weight capping indicators for logical processor types that have not yet been installed and have no reserved CPs defined.
   - Increase the reserved value for logical processor types that have not been installed and already have reserved CPs defined.
3. To have the new changes take effect immediately, click **Change Running System**.

4. To have the new changes take effect when the logical partition is activated with the modified profile, click **Save to Profiles**.
5. To have the new changes take effect immediately and also when the logical partition is activated with the modified profile, click **Save and Change**.

Logical Processor Add

This window allows you to select logical processor definitions to be changed dynamically on the system, in the image profile, or both. Dynamic changes will take effect without performing a reactivation of the logical partition. This tasks allows you to:

- Increase the initial and/or reserved values for installed logical processor type(s).
- Add a reserved value and set weight and capping indicators for logical processor type(s) that have not yet been installed and have no reserved CPs defined.
- Increase the reserved value for logical processor type(s) that have not been installed and already have reserved CP(s) defined.

The partition status (active/inactive) is indicated in the window title, along with the logical partition name. If the logical partition is active, the current settings are displayed. If the logical partition is inactive, the settings contained in the image profile will be displayed.

Logical processor add table

This table displays the logical processor assignments for the logical partition. There is one row in the table for each CP type allowed for the logical partition's mode. Input fields are enabled/disabled depending on the logical partition configuration and current settings.

CP Type
Displays the logical processor type.

Number of Initial CPs
The number of initial central processing units for the logical processor type. If the logical processor type is installed, this value can be increased.

Number of Reserved CPs
The number of reserved central processing units for the logical processor type. In order to increase this value in the profile, the logical processor type must be currently installed. If the logical processor type is not currently installed, the number can be increased in the active logical partition only.

Capping
Indicates whether or not the initial processing weight of the logical processor type is capped. When the initial processing weight is capped, it is a limit. When the initial processing weight is *not* capped, it is a target, not a limit. Initial capping can be modified only when new processor type(s) are being defined and they are non-dedicated.

Dedicated
Indicates whether or not the logical processor type is dedicated or shared within the logical partition. This field cannot be modified.

Initial Weight
The initial processing weight for the processor type. The initial processing weight can be modified only when new processor type(s) are being defined and the logical processor type is non-dedicated.

Minimum Weight
The minimum processing weight for the processor type. The minimum processing weight can be modified only when new processor type(s) are being defined and Workload Manager (WLM) is enabled for the logical partition.

Maximum Weight
The maximum processing weight for the processor type. The maximum processing weight can be modified only when new processor type(s) are being defined and Workload Manager (WLM) is enabled for the logical partition.

Additional functions are available from this window.

Save to Profiles
If you want the new settings to take effect whenever the logical partition is activated with the modified profile, click **Save to Profiles**

Saving new settings modifies the following activation profiles:

- Saves a logical partition's processor control settings in its image profile. The settings take effect whenever the logical partition is activated with its image profile.
- **Save to Profiles** can be selected for both active and inactive logical partitions. The partition status (active/inactive) is indicated in the panel title, along with the logical partition name.

Note: Saving processor controls to the image profile saves *all* the processor controls currently displayed, regardless of when the settings were made. For example, if the **Logical Processor Add** window was previously used to change some of the active partition's processor controls, those changes are saved in the profile along with any changes subsequently made.

Change Running System
If you want the new settings to take effect in the active logical partition immediately, click **Change Running System**.

Changes the processor settings in the logical partition without reactivating the partition. The new settings remain in effect for the logical partition until you either dynamically change the settings again or reactivate the partition.

Note: Change Running System can be selected for an active logical partition only. For an inactive partition, the **Change Running System** button will be disabled.

Save and Change
If you want the new settings to take effect immediately *and* whenever the logical partition is activated with the modified profile, click **Save and Change**.

Save and Change performs the combined operations of **Save to Profiles** and **Change Running System**.

Reset
To return the values back to their original values, click **Reset**.

Cancel
To close this window without saving changes you made and exit this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Capping

Use this field to set capping of the initial processing weight when defining a non-dedicated logical processor. A check indicates the logical processor's initial processing weight is capped.

For each logical processor type that is already defined, the field in this column displays the initial capping setting for the processor. If the processor is already defined, capping cannot be changed.

A logical processor's *initial weight* is its relative amount of shared processor resources. The *initial capping* setting indicates whether the logical processor is prevented from using processor resources in excess of its processing weight.

- When the initial processing weight is *not* capped, it is a target, not a limit. It represents the share of resources guaranteed to a logical processor when all processor resources are in use.
- When the initial processing weight is capped, it is a limit. It represents the logical processor's maximum share of resources, regardless of the availability of excess processor resources.

Note:

- Initial capping can be modified only when new processor type(s) are being defined and they are non-dedicated.

- Initial capping cannot be selected if the logical partition is WLM managed because they are mutually exclusive.

Initial Weight

Use this field to set the initial processing weight when defining a logical processor type that is non-dedicated.

For each logical processor type that is already defined, the field in this column displays the initial processing weight assigned to the processor. If the processor is already defined, the initial processing weight cannot be modified.

A logical processor's *initial processing weight* is its relative amount of shared processor resources.

An initial processing weight represents the share of resources guaranteed to the logical partition when all processor resources are in use. Otherwise, when excess processor resources are available, the logical partition can use them if necessary. When a logical partition is not using its share of processor resources, other active logical partitions can use them.

While excess processor resources are available, initial processing weights have no effect on how those resources are used. Instead, initial processing weights take effect only when the number of logical processors requiring a timeslice is greater than the number of available physical processors.

Note:

- The initial processing weight can be a value from 1 to 999.
- Initial processing weight can be modified only when new processor type(s) are being defined and they are non-dedicated.

Minimum Weight

Use this field to set the minimum processing weight when defining a non-dedicated logical processor and Workload Manager (WLM) is enabled for the logical partition.

For each logical processor type which is already defined, the field in this column displays the minimum processing weight assigned to the processor. If the processor is already defined, the minimum processing weight cannot be modified.

When Workload Manager is enabled, a logical partition's *minimum weight* places a lower limit on the amount of shared processor resources. The exact percentage of resources allocated to the logical partition depends on the processing weights of other logical partitions defined and activated on the central processor complex (CPC) at the same time.

- The minimum processing weight can be a value from 0 to 999. A value of 0 indicates that there is no minimum processing weight.
- The minimum weight must be less than or equal to the initial processing weight.
- Minimum processing weight can be modified only when new processor type(s) are being defined, they are non-dedicated and WLM is enabled for the logical partition.

Maximum Weight

Use this field to set the maximum processing weight when defining a non-dedicated logical processor and Workload Manager (WLM) is enabled for the logical partition.

When Workload Manager is enabled, a logical partition's *maximum weight* places an upper limit on the amount of shared processor resources. The exact percentage of resources allocated to the logical partition depends on the processing weights of other logical partitions defined and activated on the central processor complex (CPC) at the same time.

- The maximum processing weight can be a value from 0 to 999. A value of 0 indicates that there is no maximum processing weight.
- The maximum weight must be greater than or equal to the initial processing weight.

- Maximum processing weight can be modified only when new processor type(s) are being defined, they are non-dedicated and WLM is enabled for the logical partition.

Logoff or Disconnect

Accessing the Logoff or Disconnect task

This task allows you to end the current user session and logs off the Support Element console or to disconnect while your tasks continue running. If you disconnect, you can reconnect at a later time to continue working. However, a disconnected session is eventually ended. (This is because disconnected sessions exist only while the Support Element console application is running. If the Support Element console is restarted or the console is shut down or rebooted, all session information is lost.)

Select the log off operation when you no longer need access to the Support Element console. Logging off the console does not affect the status of the system. After you log off or disconnect, the Welcome to the Primary Support Element Console window is displayed. If you chose to disconnect rather than logoff, when you logon again, the Choose a Disconnected Session window is displayed. You can select the disconnected session to continue working or you can begin a new session. (The number of windows displayed depends on the state of the session when it was disconnected. One of the windows is the main user interface; additional windows are for each task that was running when the session was disconnected.)

The Support Element workplace window closes and the Hardware Management Console workplace window is displayed.

To log off the Support Element console:

1. Open the **Logoff or Disconnect** task or select **Logout** from the user ID drop down located in the upper right corner of the workplace. The Choose to Logoff or Disconnect window is displayed.
2. Select **Log off**.
3. Click **OK** to end your session on the Support Element console.

To disconnect from the Support Element console:

1. Open the **Logoff or Disconnect** task or select **Logout** from the user ID drop down located in the upper right corner of the workplace. The Choose to Logoff or Disconnect window is displayed.
2. Select **Disconnect**.
3. Click **OK** to disconnect from your session on the Support Element console with the intent of returning at a later time.

Support Element Logoff or Disconnect

This task is used to close the console workplace and log off or disconnect from the console.

Log off
To exit the console, select **Log off**.

Logging off only ends the current console session. It does *not* affect the status or operation of the defined systems or images.

Note: If you log off while tasks are active or windows are open the console will notify you that there are active tasks or open windows. You have the option to proceed, terminating all tasks that are running before they complete.

Disconnect
To disconnect from the console, while preserving your session as your tasks continue to run, select **Disconnect**.

When you log back on you will be notified of the disconnected sessions and whether or not you want to reconnect to them or begin a new session.

OK
To continue with the selection you made, click **OK**.

Cancel
To close the window without logging off or disconnecting from the console, click **Cancel**.

Help
To display help for the current window, click **Help**.

Logon

Support Element Logon

This window is used to specify your user credentials for logging on to the console:

- User identification (username)
- Password
- Authentication code, if required

Your username, password, and whether you require Multi-factor Authentication (MFA) enablement are assigned to you initially by your access administrator. Afterward, you can change your password while logging on to the console. If you do not know your username and password, contact your access administrator or whoever is responsible for controlling access to the console.

Note: If your password expires, you are prompted to change it.

Username
Specify the string of characters that identifies you to the console.

Password
Specify the string of characters that verifies your user identification and your authority to log on the console.

Note: Your password is not displayed. Black dots are displayed as you type your password.

Use authentication code
Select this option if your username is MFA-enabled and if SE MFA has been previously set up.

LOGIN (with MFA)
If your username is MFA-enabled, log on to this console by using the following procedure.

1. Specify your username in the **Username** input field.
2. Specify your password in the **Password** input field.
3. Select **Use authentication code** if you have previously set up SE MFA and enter your authentication code in the **Authentication code** input area.
4. Click **LOGIN**.
5. If this is the first time you are logging in to the console, the *Secure your account with multi-factor authentication* window is displayed. Proceed with the "Setting up Time-based One-Time Password Multi-factor Authentication" on page 654 section.
6. To exit your session and close the window, select the **Logoff or Disconnect** task, click the **X** in the upper right of the window, or click your user ID from the masthead and select **Logout**.

LOGIN (without MFA)
If your username is not MFA-enabled, log on to this console by using the following procedure.

1. Specify your username in the **Username** input field.
2. Specify your password in the **Password** input field.
3. Click **LOGIN**. The **Support Element Console Workplace** is displayed.
4. To exit your session and close the window, select the **Logoff or Disconnect** task, click the **X** in the upper-right corner of the window, or click your user ID from the masthead and select **Logout**.

Cancel
To close the window without logging on to the console, click **Cancel**.

HELP
To display help for the current window, click **HELP**.

Setting up Time-based One-Time Password Multi-factor Authentication

If your access administrator requires you or other users to use the Time-based One-Time Password (TOTP) multi-factor authentication to log on to the console, continue with the following steps the first time you log on to the console. The access administrator sets the SE MFA setting from the **User Management** task.

1. Provide your user name and password on the logon window, then click **LOGIN**.
2. You will begin the multi-factor authentication set up, the *Secure your account with multi-factor authentication* window is displayed, click **NEXT**.

   At any point during this multi-factor authentication process, you can use the following options that appear on the windows:

   Cancel Setup
   To leave this window without logging on to the console, click **Cancel Setup**. A window is displayed verifying that you want to cancel the setup of the multi-factor authentication. Click **YES** to return to the logon window or click **NO** to continue with the set up.

   NEXT
   To continue with multi-factor authentication, click **NEXT**.

   BACK
   To go back to the previous window, click **BACK**.
3. The *Install an authentication app on your mobile device* window is displayed.
4. Install the Google Authenticator app (or any compatible app) on your mobile device. This is a supported multi-factor authentication app for logging on to the console. Once you have installed the app on your mobile device, click **NEXT**.
5. The *Scan the bar code with your authentication app* window is displayed.
   - If you choose to scan the bar code, use your mobile device to scan the code displayed in the window and receive your one-time-use password from the app on your mobile device.
   - You can select **View text code instead** and use the key that appears on the *Enter the following key in your authentication app* window. Provide this key to the app on your mobile device to receive the one-time-use password.
6. After receiving your one-time-use password from the authentication app, click **NEXT**, the *Enter your authentication code* window is displayed.
7. Enter your one-time-use password in the authentication code field, then click **NEXT**. The *Success! Multi-factor authentication is now enabled* window is displayed.

   Notes:

   - Your one-time-use password changes every 30 seconds.
   - The console accepts the one-time-use password for the current, previous, and next 30-second interval, according to its clock.
     - That allows some time for you to enter the authentication code, and it allows for some discrepancy between the mobile device clock and the console clock.

The next time you logon to the console, you will only need to enter your user name, password, and the current authentication code from the app on your mobile device.

LPAR Internal Code Change Utility

LPAR Internal Code Change Utility

Use this window to work with partition internal code changes, to temporarily change or fix the internal code image that supports the operating mode of the selected object.

You can use the partition internal code change utility to work with up to ten partition internal code changes at once.

You can find more detailed help on the following elements of this window:

Options Menu

Use the **Options** menu to work with a partition internal code change.

Apply now
To immediately apply the selected partition internal code change to the internal code image of the selected object.

Remove now
To immediately remove the selected internal code change from the internal code image of the selected object.

Never automatically apply during activation
To set the selected partition internal code change to not be applied automatically when the selected object is activated.

Always automatically apply during activation
To set the selected partition internal code change to be applied automatically every time the selected object is activated.

Automatically apply only during the first activation
To set the selected partition internal code change to be applied automatically the next time the selected object is activated, but not for any subsequent activation.

Delete a change from the list of available choices
To delete the selected internal code change from the list of changes currently managed by the partition internal code change utility.

Add a new change to the list of available choices
To add an internal code change to the list of changes currently managed by the partition internal code change utility.

Exit
To end this task and return to the Support Element Workplace window.

Internal Code Change Utility List

This list displays the partition internal code changes currently managed by the partition internal code change utility. Select an internal code change to work on, then select a choice from the **Options** menu.

Change
Indicates the partition internal code changes currently managed by the partition internal code change utility.

Type
Indicates whether a partition internal code change can be applied to a system operating in logically partitioned mode , or to a logical partition operating in coupling facility mode.

Automatic Application
Indicates whether a partition internal code change is set to be applied automatically to the selected object when the object is activated.

Status
Indicates whether a partition internal code change is currently applied to the selected object.

Status Reason
Displays a brief explanation of the reason for the current status of a partition internal code change.

Comment
Displays a short description, if available, of a partition internal code change.

Change

This column identifies the partition internal code changes currently managed by the partition internal code change utility.

A change can be identified by:

A four digit number
Identifies the partition internal code change.

This number is also the last four characters in the eight character name of the source file for the partition internal code change.

In use
Indicates the partition internal code change is currently managed by this utility, but it does not support the operating mode of the selected object.

You cannot use choices from the **Options** menu to work on changes that are in use.

Type

This column indicates whether the partition internal code change can be applied to a system operating in logically partitioned mode , or to a logical partition operating in coupling facility mode.

The type can be:

Coupling facility
Indicates the internal code change can be applied only to a logical partition operating in coupling facility mode.

Partitioned
Indicates the internal code change can be applied only to a system operating in logically partitioned mode.

Automatic Application

This column indicates whether a partition internal code change is set to be applied automatically to the selected object when the object is activated.

The automatic application setting can be:

Never
Indicates the internal code change will not be applied any time the object is activated.

Always
Indicates the internal code change will be activated every time the object is activated.

Once
Indicates the internal code change will be applied the next time the object is activated. Afterwards, the setting will change automatically to **Never**.

Status

This columns indicates whether a partition internal code change is currently applied to the selected object.

The status can be:

Active
Indicates the internal code change currently is applied.

Inactive
Indicates the internal code change currently is not applied.

Status Reason

This column displays a brief explanation of the reason for the current status of a partition internal code change.

The reason can be:

Applied at partition activation
When the internal code change status is **Active**, this reason indicates the internal code change was automatically applied successfully by the most recent activation.

Applied by request
When the internal code change status is **Active**, this reason indicates the internal code change was applied successfully using the **Applied now** choice on the **Options** menu.

Applied during power-on reset
When the internal code change status is **Active**, this reason indicates the internal code change was automatically applied successfully by the most recent power-on reset.

Apply failed
When the internal code change status is **Inactive**, this reason indicates the internal code change was not applied successfully.

CF partition activation required
When the internal code change status is **Inactive**, this reason indicates the selected logical partition is not operating in coupling facility mode.

Change statement error
When the internal code change status is **Inactive**, this reason indicates the internal code change could not be applied, or could not be set for automatic application, because the internal code change includes at least one statement that is not valid.

Logically partitioned mode required
When the internal code change status is **Inactive**, this reason indicates a power-on reset is complete, but the selected system is not operating in logically partitioned mode.

New change
When the internal code change status is **Inactive**, this reason indicates the internal code change is new, and has not yet been worked on using the choices on the **Options** menu.

Power-on-reset required
When the internal code change status is **Inactive**, this reason indicates a power-on-reset of the selected system was not performed or is not complete.

Remove failed
When the internal code change status is **Active**, this reason indicates the internal code change was not removed successfully.

Removed by request
When the internal code change status is **Inactive**, this reason indicates the internal code change was removed successfully using the **Remove now** choice on the **Options** menu.

(blank)
When the internal code change status is **Inactive**, this reason indicates the internal code change was not applied during the most recent activation of the selected object, and has not yet been worked on using the choices on the **Options** menu.

OK

To perform the selected internal code change, click **OK**.

Cancel

To close the window, click **Close**.

Help

To display help for the current window, click **Help**.

Apply now

To immediately apply the selected partition internal code change to the current internal code image, select this menu choice.

Before applying an internal code change:

1. Check the **Change** column to verify it does not display **In use** for the selected partition internal code change.
2. Check the **Type** column to verify the type of the selected partition internal code change matches the operating mode of the selected object.
3. Check the **Status** column to verify the status of the selected partition internal code change is **Inactive**.

Remove now

To immediately remove the selected partition internal code change from the current internal code image, select this menu choice.

Removing a partition internal code change undoes its application to the internal code image. After it is removed, an internal code change is no longer working part of the internal code image that supports the operating mode of the selected object.

Before removing an internal code change:

1. Check the **Change** column to verify it does not display **In use** for the selected partition internal code change.
2. Check the **Type** column to verify the type of the selected partition internal code change matches the operating mode of the selected object.
3. Check the **Status** column to verify the status of the selected partition internal code change is **Active**.

Delete a change from the list of available choices

To delete the selected partition internal code change from the list of changes currently managed by the partition internal code change utility, select this menu choice.

Before deleting a partition internal code change:

1. Check the **Change** column to verify it does not display **In use** for the selected partition internal code change.
2. Check the **Status** column to verify the status of the selected partition internal code change is **Inactive**.

Deleting the change does not erase its source file from the Support Element hard disk. Deleting the change only removes it from the group of changes you can work with using the utility.

Add a new change to the list of available choices

To add a partition internal code change to the list of changes currently managed by the partition internal code change utility, select this menu choice.

Before adding a partition internal code change, check the **Change** column to verify the change is not currently managed by the utility.

Note: You can edit the source file of a change currently managed by the utility. But to work with the new copy of the change, you must remove and delete the copy of the change currently listed, then add the edited copy as a new change.

Another panel displays for you to specify the number that identifies the internal code change.

Partition Internal Code Change

Use this window to type the number that identifies the partition internal code change you want to add.

Partition internal code changes are identified by a 4 digit decimal number from 0000 through 9999. This number is also the last four characters in the eight character name of the source file for the partition internal code change.

The source file must be named as follows:

- The first 4 characters of the file name must be IQZQ.
- The last 4 characters of the file name must be a number from 0000 through 9999.
  - Logical partition internal code changes have identifiers in the range from 0000 through 4999.
  - Coupling facility internal code changes have identifiers in the range from 5000 through 9999.
- The file type must be TRM.

You can find more detailed help on the following elements of this window:

Change Identifier

Type the change identifier of the partition internal code change you want to add to the changes currently managed by this utility.

- Type an identifier in the range from 0000 through 4999 to add a logical partition internal code change.
- Type an identifier in the range from 5000 through 9999 to add a coupling facility internal code change.

OK

To perform the selected internal code change, click **OK**.

Cancel

To close the window, click **Close**.

Help

To display help for the current window, click **Help**.

Object

The tasks you perform while using this partition internal code change utility will temporarily change or fix the internal code image that supports the operating mode of the object you selected on the **Support Element Workplace** window.

The object can be:

- A system operating in logically partitioned mode.
- A logical partition operating in coupling facility mode.

Activation

Activation is a sequence of operations performed to make an object operational.

To automatically apply an internal code change to logical partitioning internal code, activation must include successful completion of a power-on reset of the system in logically partitioned mode.

To automatically apply an internal code change to coupling facility control code, activation must include successful completion of partition activation of a logical partition operating in coupling facility mode.

Partition Internal Code Change

A partition internal code change temporarily changes or fixes the image of the internal code that supports the operating mode of an object.

There are two types of partition internal code change:

Logical partitioning internal code change
An internal code change for the internal code image that supports operating a system in logically partitioned mode (LPAR mode).

Coupling facility internal code change
An internal code change for the internal code image that supports operating a logical partition in coupling facility mode.

Internal Code Image

The internal code image is a copy of the internal code that supports the operating mode of an object.

The internal code is stored on the support element of the central processor complex (CPC) that provide processing resources for the object. An image of that internal code is loaded into processor storage when the object is activated.

Apply

Applying an internal code change makes it a working part of the internal code image that supports the operating mode of an object.

The internal code is stored on the Support Element of the central processor complex (CPC) that provide processing resources for the object. An image of that internal code is loaded into processor storage when the object is activated.

Note: The partition internal code change is applied only to the image loaded into processor storage. Applying a partition internal code change does not modify the internal code stored on the support element.

Manage Adapter Firmware

Accessing the Manage Adapter Firmware task

Use this task to select a condition to either:

- Query adapters currently requiring a configure off/on action in order to perform a code load.
- Query adapters that require a configure off/on action after the next install and activate of an adapter in order to perform a code load.

To query adapters that are configure off/on pending:

1. Locate the **CPC** to work with.
2. Open the **Manage Adapter Firmware** task.

   The Manage Adapter Firmware window displays.
3. Click **Manage current updates** to display a list of adapter that have configure off/on current conditions pending.
4. Click **Manage updates after install and activate** to display a list of adapters that have configure off/on conditions pending in the next nondisruptive code load.

Manage Adapter Firmware

Use this window to select a condition to either:

- Query adapters that are currently have pending a configure off/on action in order to perform a code load
- Query adapters that will require a configure off/on action after the next install and activate of a adapters in order to perform a code load.

Manage current updates
To display a list of adapters that are currently pending a configure off/on action to perform a nondisruptive adapters code load, click **Manage current updates**.

Manage updates after install and activate
To display a list of adapters that require a configure off/on action in the next nondisruptive code load, click **Manage updates after install and activate**.

Cancel
To close the window and exit the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Manage Adapter Firmware

Use this window to review and select from the list of channel and crypto adapters that are currently pending a configure off/on action in order to complete a nondisruptive adapter code load.

Adapter Firmware Information
The table lists the following information for the current active adapters that are pending a configure off/on action in order to perform a code load.

Adapter
Displays the four-digit physical channel identifier of each adapter

ID
Displays a two-digit number that is a channel path identifier of each channel path and the crypto number displays the number assigned to the crypto.

Active EC/MCL
Displays the current active code in the adapter

Pending EC/MCL
Displays the pending code to be loaded into the adapter after a configure off/on

Adapter type
Displays the channel or crypto type for the assigned adapter

Type
Displays the specific type of channel or the specific type of crypto.

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Update firmware
Performs an adapter firmware update on the selected channel and cryptos.

The icons perform the following functions in the adapter table:

Select All
Selects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Deselect All
Deselects all objects in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header to change from ascending to descending order. Click **OK** when you have defined your preferred order.

Show Filter Row

Defines a filter for a table column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the check box next to the filter that you want in the filter row.

Clear All Filters

Returns to the complete table summary. The table summary includes the total number of items that pass the filter criteria and to the total number of items.

Clear All Sorts
Returns the table back to the default order.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Close
To close the window and exit the task, click **Close**.

Help
To display help for the current window, click **Help**.

Manage Adapter Firmware

Use this window to review a list of active adapters with an assigned physical channel identifier (PCHID) that are pending a configure off/on action in the next install and activate of a nondisruptive adapter code load.

Adapter Information
The table lists the following information for the current active adapters that are pending a configure off/on action to perform a code load.

Adapter
Displays the four-digit physical channel identifier of each adapter.

ID
Displays a two-digit number that is a channel path identifier of each channel path and the crypto number displays the number assigned to the crypto.

Adapter type
Displays the channel or crypto type for the assigned adapter.

Type
Displays the specific type of channel or the specific type of crypto.

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears. The icons perform the following functions in the adapter table:

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header to change from ascending to descending order. Click **OK** when you have defined your preferred order.

Show Filter Row

Defines a filter for a table column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the check box next to the filter that you want in the filter row.

Clear All Filters

Returns to the complete table summary. The table summary includes the total number of items that pass the filter criteria and to the total number of items.

Clear All Sorts
Returns the table back to the default order.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Close
To close the window and exit the task, click **Close**.

Help
To display help for the current window, click **Help**.

Adapter target list not valid

Use this window to view the list of adapters that are not supported for a firmware update.

Adapter Name
Displays the unsupported adapter(s) name for the firmware update.

Reason
Displays the reason the unsupported adapter(s) for the firmware cannot be updated at the current time.

Additional functions on this window include:

Yes
To continue updating the supported adapters for the firmware update, click **No**.

No
To return to the previous window, click **Yes**.

Help
To display help for the current window, click **Help**.

Manage Firmware Features

Accessing the Manage Firmware Features task

The **Manage Firmware Features** task allows you to view the current enablement status of all firmware features and to enable or disable those features. The task enables a firmware feature by importing a feature definition file from a Support Element USB or from an FTP server.

A feature definition file contains metadata for a feature including additional actions, if any, required to enable it.

To enable firmware features:

1. Locate and open the **Manage Firmware Features** task. The Manage firmware features window displays.
2. Click **Import** from the **Firmware features** window to enable a firmware feature by importing a feature definition file from a Support Element USB media or from an FTP server.

   Firmware features requiring additional actions remain Enable pending status until additional actions are performed.

Manage PCI System Services

Accessing Manage PCI System Services task

To manage the PCI Resource Group:

1. Open the **Manage PCI System Services** task.

   The Manage PCI System Services window displays.

Manage PCI System Services

Use this window to manage the PCI Resource Groups to:

- Perform an activation of a PCI Resource Group that is not operating.
- Perform an update to a PCI Resource Group.

PCI system service table:

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Select
Indicates the PCI Resource Group selected.

Target
Indicates the PCI Resource Group.

Status
Indicates the current status of PCI Resource Group.

Partition Changes Pending Install and Activate
Indicates there are staged MCL updates which causes the Update Pending condition once an Install/Activate is performed for the selected PCI Resource Group. It is recommended to use the **Change Internal Code** task prior to updating the selected PCI Resource Group.

Note: This column displays for SERVICE mode only.

Update Pending
Indicates an update is pending for the selected PCI Resource Group. The selected PCI Resource Group must be operating.

The icons perform the following functions in the PCI Resource Group table:

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

PCHIDs defined table:

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

PCHID
Indicates the PCHID that is affected by a disruptive update to the selected PCI Resource Group.

State
Indicates the current state of the PCHID.

Status
Indicates the status of the PCHID.

Partition
Indicates the owning partition for this PCHID.

Partition Status
Indicates the current status of the owning partition.

The icons perform the following functions in the PCHIDs defined table:

Export Data
Downloads table data in a Comma Separated Values (CSV) file. You can then import this downloaded CSV file into most spreadsheet applications.

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want.

Clear All Filters
Click **Clear All Filters** to return to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Cancel
To exit the current task, click **Cancel**.

Help
To display help for the current window, click **Help**.

PCI Resource Group Update

This window displays all Online ID(s) and their associative partitions that will be affected during this PCI Resource Group disruptive update. It is recommended that you verify these ID(s) redundancy prior to performing the update. Use the **Configure On/Off** task to configure the Channel and Function ID (FIDs).

Channel and FIDs online table

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

ID
Indicates the ID that is affected by the PCI Resource Group disruptive update

State
Indicates the operational state of the ID

Status
Indicates the status of the ID

Type
Indicates the adapter type of ID

Partition
Indicates the owning partition of the ID

Partition Status
Indicates the current status of the owning partition

PCHID
Indicates the PCHID the ID is mapped to.

The icons perform the following functions for the FIDs Online table:

Export Data
Downloads table data in a Comma Separated Values (CSV) file. You can then import this downloaded CSV file into most spreadsheet applications.

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want.

Clear All Filters
Returns to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
The **Edit Sort** button is used to perform multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, single column sorting can be performed by selecting the **^** in the column header to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Update Resource Group Firmware
To continue with the update resource group process, click **Update Resource Group Firmware**.

Cancel
To exit the current task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Manage Print Screen Files

Accessing the Manage Print Screen Files task

This task allows you to create screen captures of the entire contents of the console or of individual task windows. You can then manage these files by viewing, copying to media, or deleting.

To capture and manage the print screen files:

1. Open the **Manage Print Screen Files** task. The Manage Print Screen Files window is displayed.
2. Specify a file name and select a file type from the list that you prefer to have the screen capture saved as.
3. You can capture a window or screen by clicking one of the following options:

   Print Window
   Creates a copy of a task window and gives it a unique file name and the selected file type. A message window is displayed explaining how to get the preferred window to the foreground.

Print Screen
Creates a copy of the entire contents of the screen and gives it a unique file name and the file type you selected. A message window is displayed explaining the amount of time you have to arrange the windows on the screen before it is captured.

Your screen capture is displayed in a table within the task window once the process is complete.

4. You can select a file from the table and then proceed with an option to view the file, copy the file to media, convert to a different file type, delete the file, or rename the file.
5. When you are done and ready to exit, click **Cancel**.

Manage Print Screen Files

Use this task to manage the console's print screen files.

This window lists the print screen files which currently exist on the console. If no files currently exist then the list will be empty.

You can select one or more files from the list, then click **View...**, **Copy...**, **Convert**, or **Delete** to perform that action on the selected file or files. If copying or converting a single file, you can specify a new file name as well.

You can select one file from the list, specify a new file name, then click **Rename** to rename the selected file.

To create new print screen files for the specified file name and file type, click **Print Window** or **Print Screen**. If a file name is not specified, a system generated file name will be used.

File name
To assign a file name for the print screen file, specify up to twenty alphanumeric characters. When creating a print screen file, if a file name is not specified a system generated name will be used. The file name can be specified when copying, converting, renaming or creating a print screen file.

Note: This option is not available when you are accessing the console remotely and no print screen files exist.

File type
To assign a file type of the print screen file, select the down arrow for a list of supported file types, then click on one of the file types in the list to select it.

Note: This option is not available when you are accessing the console remotely and no print screen files exist.

View...
To view one or more print screen files, select the files, then click **View...**. This displays the View Print Screen Files window.

Note: This option is not available if print screen files do not exist.

Copy...
To copy one or more print screen files to media, select the files, then click **Copy...**. The **Select Media Device** window is displayed where you can choose the media to which the files will be copied. If there is enough space available on the media, the files will be copied to that media. If files already exist on the media with the same file name as the selected files, the files on the media will be replaced with the selected files. If just one print screen file is selected, a file name can be specified to give the copied print screen file a new file name.

Note: This option is not available when you are accessing the console remotely or if no print screen files exist. On a remote session screen where files do exist, right click on the thumbnail to save it locally.

Convert
To convert one or more print screen files, select the files and select the file type, then click **Convert**. Selected print screen files which are already of the selected file type will be ignored. If just one print

screen file is selected, a file name can be specified to give the converted print screen file a new file name.

Note: This option is not available if no print screen files exist.

Rename
To rename a print screen file, select the file, specify a new file name, then click **Rename**.

Note: This option is not available if no print screen files exist.

Delete
To remove one or more print screen files, select the files, then click **Delete**. You are prompted to confirm the delete to ensure the files are not deleted accidentally.

Note: This option is not available if no print screen files exist.

Print Window
To create a print screen file for a specific window, click **Print Window**. A message is displayed that explains how to use the Alt+Tab keyboard keys to get the window you want to come to the foreground. Then move the mouse cursor, which has changed to crosshairs, to any spot on that window and click on the window to create the print screen file. The list of files is updated to include the new print screen file.

Note: This option is not available when you are accessing the console remotely.

Print Screen
To create a print screen file for the entire screen, click **Print Screen**. A message is displayed that explains that you have a set amount of time to use the Alt+Tab keyboard keys to arrange the windows on the screen before the print screen file is created. The list of files is updated to include the new print screen file.

Note: This option is not available when you are accessing the console remotely.

Refresh
To refresh the list of print screen files, click **Refresh**. If you create print screen files using Alt+Print Screen or Shift+ Print Screen, then click **Refresh** to get the list of files updated. Shift+Print Screen prints the entire screen to a file, Alt+Print Screen selects a specific window to print to a file.

Note: You cannot use the Shift+Print Screen or Alt+Print Screen keyboard functions if you are accessing the console remotely.

OK
To save your changes, click **OK**.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

View Print Screen Files

Use this window to view one or more print screen files. If more than one file is selected, the files are displayed in a tabbed format, with the file names displayed on the tabs. When large window or full screen files are displayed you may need to use the window scroll bars to navigate throughout the window.

Cancel
To close the view print screen files window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Select Media Device

Use this window to select the device to which the files will be copied.

OK
To continue the task with the selected media, click **OK**.

Refresh
To update the device list, click **Refresh**.

Cancel
To exit this window without making any changes and to return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Manage Product Engineering Access Control File

Accessing the Manage Product Engineering Access Control File task

This task is used by a service representative or a user that has service representative task roles access. Use this task to import an access control file which allows product engineering access to this console.

1. Open the **Manage Product Engineering Access Control File** task. The Manage Product Engineering Access Control File window is displayed.
2. Select the location of the access control file you want to import.

   Note: The options for importing the access control file depend upon how you are accessing the console.
3. Click **IMPORT** to import the specified access control file.

Manage Product Engineering Access Control File

Use this window to specify the location of the access control file.

If you are accessing this task locally on the console, select the location of the access control file from an FTP server or from removable media.

If you are accessing the console remotely, select the location of the access control file from an FTP server or from a remote file system.

FTP server
To select a file from an FTP sever, select **FTP server**. Provide the following information if you are providing an access control file from an FTP server.

Host name:
Specify the host name address or destination. This is a required field.

User name:
Specify the user name for the target FTP destination. This is a required field.

Password:
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol:

Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)
- **SFTP** (SSH File Transfer Protocol)

Removable media
To import the access control file from a USB flash memory drive, select **Removable media**. To see a list of the available USB flash memory drives, use the drop-down and then select the USB flash memory drive for importing the access control file. To make sure you have the currently available USB flash memory drives, click **Refresh**. This option is only available when this task is accessed locally on the console.

Note: If you're using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

File system
To select the access control file from a remote file system, select **File system**.

Note: This option is only available if you are accessing the console remotely.

Control file:
Specify the file name of the access control file or click **BROWSE** to select the access control file that you want to import.

CANCEL
To close this window and end the task without importing an access control file, click **CANCEL**.

IMPORT
To import the selected access control file, click **IMPORT**.

HELP
To display help for the current window, click **HELP**.

Manage Remote Support Requests

Accessing the Manage Remote Support Requests task

This task views or manages call-home requests that the console has submitted.

1. Open the **Manage Remote Support Requests** task. The Manage Remote Support Facility Requests window is displayed.
2. This window lists active requests (being transmitted) and waiting requests. You can select requests in the lists. You can display options by clicking **Options** on the menu bar. The options permit you to:
   - View all Support Elements that are configured as call-home servers for this console
   - Cancel selected requests
   - Cancel all active requests (those being transmitted)
   - Cancel all waiting requests
   - Close the window and exit.
3. Select **Options** (from the menu bar), **Exit** when you have completed the task.

Manage Remote Support Facility Requests

Use this window to view or manage call-home requests submitted by the console that are either being processed or waiting to be processed.

Click **Options** on the menu bar to:

- **"View All Call-Home Servers" on page 671** to view a list of all consoles that are configured as call-home servers for this console.
- **Cancel Selected Requests** to remove the selected request from the list.
- **Cancel All Active Requests** to cancel all requests in the Active Requests list.
- **Cancel All Waiting Requests** to cancel all requests in the Waiting Requests list.
- **Exit** to close this window and return to the console workplace.

Click **Help** on the menu bar to display help for the current window.

Active Requests

The Active Requests table provides the following information about call-home requests being processed:

Status
The status of a request that is being processed can be:

Submitted
This request has been accepted and processing for it is being arranged (on either this machine or another machine).

Handling
The request is being processed.

Canceling
Someone has canceled this request.

Reporting
The result of the request is reported back through the programming interface to the submitter.

Call-Home Server
The actual machine where the call-home request is being processed. A call-home server is a console that provides internet connectivity to request service or transmit hardware serviceability data to the support system.

Date
The date the call-home request was submitted.

Time
The time the call-home request was submitted.

Description
A brief description of the request from the programming interface through which it was submitted.

Waiting Requests

The Waiting Requests table provides the following information about call-home requests waiting for processing:

Date
The date the call-home request was submitted.

Time
The time the call-home request was submitted.

Description
A brief description of the request from the programming interface through which it was submitted.

View All Call-Home Servers

Use this window to view a list of all consoles that are configured as Call-Home Servers for this console.

Monitors Dashboard

Accessing the Monitors Dashboard task

Use this task to monitor system activity and display activity details for this system.

To monitor system activity for your system:

1. Open the **Monitors Dashboard**. The Monitors Dashboard window is displayed. The overview table includes information on machine type and model, processor and I/O usage, power consumption, and ambient air temperature. Expand the Details section to view activity details for the system. You can also click on the Details Settings icon for a list of details that are defined for the system.
2. When you have finished viewing this information, click **Close**.

Monitors Dashboard

Use this window to monitor system activity and display activity details for this system. The activity data is automatically refreshed every 15 seconds. A blank in any table cell means that the data is not supported or not available. This is not considered an error. The local time (last refresh time and time zone) is displayed at the top window.

Select **Pause Refresh/Resume Refresh** to suspend or resume the automatic refresh of activitydata that is displayed on the current window.

Additional functions on this window include:

Close
To exit this task, click **Close**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Overview Table

The **Overview** table displays system activity data for this system. The **Overview** table displays the following information:

Name
Displays the names of the CPC.

Status

Displays the current status of the objects. Click the Hardware Messages or Acceptable Status icons in the Status column to display Hardware Message details or Acceptable Status.

Type
Displays the system type.

Machine Type - Model
Displays the machine type - model of the system.

Processor Usage
Displays a value that is the simple average of the percentages of processing capacity for ALL the physical processor lines.

I/O Usage
Displays a simple average of the percentages of I/O capacity for ALL the channel lines and adapters in the system.

Power Consumption
Represents the average power consumption of the total system over the last sampled period. The power consumption is displayed in both kilowatts (kW) and Btu per hour (Btu/hr).

Ambient Temperature
Represents the average measured temperature of the air entering the system over the last sampled period.

The toolbar at the top of the **Overview** table contains icons to select, filter, and sort the Overview table. If you place your cursor over an icon, the icon description is displayed.

The icons perform the following functions:

Select All
Selects all the systems in the **Overview** table.

Deselect All
Deselects all the systems in the **Overview** table.

Export Data
Downloads table data in a Comma Separated Values (CSV) file. You can then import this CSV file into most spreadsheet applications.

Note: This function is available only when you are accessing the Hardware Management Console or Support Element remotely.

Show Filter Row
Defines a filter for a table column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the check box next to the filter that you want in the filter row.

Clear All Filters
Returns to the complete table summary. The table summary includes the total number of items that pass the filter criteria and to the total number of items.

Edit Sort
Performs multicolumn sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, single-column sorting by selecting the ^ in the column header to change from ascending to descending order.

Clear All Sorts
The **Clear All Sorts** icon allows you to return to the default ordering.

Quick Filter
Use the quick filter function to enter a filter string in the Filter input field, and then press Enter to apply the filter. By default all the columns are filtered, showing only rows containing a cell whose value includes the filter text. Clicking the arrow displays a menu that restricts the columns to which the filter is applied.

In addition, the **Select Action** list contains actions that you can perform on the systems in the **Overview** table:

- Select **Set Thresholds** to set system activity thresholds for this system. All systems are used if there is no selection made.
- Select **Start History** to display a histogram view of system activity in various intervals and durations. A histogram is displayed for each system. All systems are used if there is no selection made.
- Select **Export Data** to download the **Overview** table data in a Comma Separated Values (CSV) file. This downloaded CSV file can be imported into most spreadsheet applications.

  Note: This function is available only when you are accessing the Hardware Management Console or Support Element remotely.

Details

The Details section is an expandable section that displays activity details for the system.

The following Details are supported:

- Power Consumption
- Environmentals
- Aggregated Processors
- Processors
- System Assist Processors
- Logical Partitions
- Channels
- Adapters

You can use the **Details** icon to select Details Settings:

- Select the **Details** icon to configure the tables for the Monitors Dashboard Details area for this system. All systems are used if there is no selection made.

You can work with the **Details** tables by using the **Select Action** list from the table tool bar.

Select **Start History** to display a view of system activity in various intervals and durations. A histogram is displayed for each selection made on the **Details** table.

Select **Processor Usage by Key** from the Processors list to display additional processor supervisor and problem states.

The following Table Actions are available:

Select All
Selects all objects in the **Details** table.

Deselect All
Deselects all selected objects in the **Details** table.

Export Data
Downloads table data in a Comma Separated Values (CSV) file. This downloaded CSV file can then be imported into most spreadsheet applications.

Show Filter Row
Defines a filter for a table column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the check box next to the filter that you want in the filter row.

Clear All Filters
Returns to the complete table summary. The table summary includes the total number of items that pass the filter criteria and to the total number of items.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, you can perform single-column sorting by selecting the ^ in the column header to change from ascending to descending order.

Clear All Sorts
Returns to the default ordering.

Quick Filter
Specifies a filter string to apply. Enter string in the **Filter input** field, and then press **Enter** to apply the filter. By default all the columns are filtered, showing only rows containing a cell whose value includes the filter text. Clicking the arrow displays a menu that restricts the columns to which the filter is applied.

Power Consumption

Displays the average power consumption over the last sampled period for the system. The power consumption is displayed in both kilowatts (kW) and Btu per hour (Btu/hr). The table also includes:

- **Total Partition Power Consumption**: The power utilized by components assigned to individual partitions.
- **Total Infrastructure Power Consumption**: The power of infrastructure components (including top of rack switches, SE/HMAs and PDUs) and should not be accounted to partition power.
- **Total Unassigned Power Consumption**: The power of unused I/O adapters and components that are not assigned to any partition (including standby components).

Power consumption also displays the line currents for the power cord data in service representative mode.

Environmentals

Displays the average ambient temperature humidity, and dew point for the system. The ambient temperature represents the average measured temperature of the air entering the system over the last sampled period. The ambient temperature is displayed in both degrees Celsius (ºC) and degrees Fahrenheit (ºF).

The humidity specifies the amount of water vapor in the air as measured by the system. The humidity sensor gives a reading of the relative humidity of the air entering the system. The recommended long-term relative humidity for a system with an altitude from sea level to 900 meters (2953 feet) is 60%. The range of acceptable relative humidity is 8% - 80%.

The dew point specifies the air temperature in degrees Celsius (ºC) and degrees Fahrenheit (ºF) at which water vapor will condense into water. This is a calculated value based on the current temperature and relative humidity. Cooling the system to the dew point can result in condensation on critical internal parts, leading to equipment failure, unless the computer room environment is adequately maintained to prevent it.

Environmental also displays the air pressure in hectopascal (hPa) in service representative mode.

Aggregated Processors

Displays the aggregated processor usage for each type of physical processor on the system. For each type of processor the table displays the aggregated processor usage for all processors and all shared processors.

Some systems have only general purpose processors, but some systems can have special processors, which can include any combination of the following:

- Integrated Coupling Facility (ICF) processors
- Integrated Facility for Linux (IFL) processors
- z Integrated Information Processors (zIIPs)

Processors

Displays the processor usage for each physical processor on the system.

Simultaneous multithreading (SMT) usage and thread usage displays showing percentage usage of each thread when the processor is running in SMT mode.

Select **Processor Usage by Key** from the Processors list to display the Processor Usage by Key window with additional processor supervisor and problem states.

Processor Usage by Key

This window displays additional data for processor's activity.

Key
Specifies the list of Program Status Word (PSW) keys for the processor. The hexadecimal list is X'0' to X'F'.

Total Usage (%)
Displays the total percentage usage for the processor's activity.

Supervisor State Usage (%)
Displays the supervisor state usage for the processor's activity.

Problem State Usage (%)
Displays the problem state usage for the processor's activity.

Additional functions on this window include:

OK
To close the current window after viewing the information, click **OK**.

Help
To display help for the current window, click **Help**.

System Assist Processors

Displays the processor usage for each System Assist Processor (SAP) on the system.

Logical Partitions

Displays the processor usage for each active logical partition on the system.

The processor usage by processor type displays and indicates processor boost status. Some systems have only general purpose processors, but some systems can have special processors, which can include any combination of the following:

- Integrated Coupling Facility (ICF) processors
- Integrated Facility for Linux (IFL) processors
- z Integrated Information Processors (zIIPs)
- Power Consumption
- Recovery Boost

If a logical partition's processing weight is not capped, its processing weight is the *minimum* share of non-dedicated processing resources guaranteed to the logical partition when all non-dedicated processing resources are in use. But when non-dedicated processing resources are available, the logical partition can borrow them, if necessary, in excess of the share ordinarily provided by its processing weight.

The Processor Usage bar range for displaying activity graphically is 0% to 100%. Actual amounts of normalized processing activity that exceed 100% are not displayed on the Processor Usage bar, but the actual processor usage value is displayed and can be greater than 100%.

Channels

Displays CSS.CHPID and the name of the owning logical partition or

```
Shared
```

if the channel is shared across partitions and the channel usage for each channel on the system.

Adapters

Displays the channel assignment, adapter type, and usage for each Crypto , Flash, and RoCE adapter on the system.

Details Settings

Use this window to configure the tables for the **Monitors Dashboard** Details area for this system. Select the tables you want to display and clear the tables you want to hide. The Details Settings are saved for the user ID.

When you start the **Details Settings** task, the current Details Settings, if any were previously saved, are displayed. Otherwise, all details tables are displayed.

Note: The default is to display all details tables.

Power® Consumption

Specifies displaying or hiding the **Power Consumption** details.

Environmentals

Specifies displaying or hiding the **Environmentals** details table.

Aggregated Processors

Specifies displaying or hiding the **Aggregated Processors** details table.

Processors

Specifies displaying or hiding the **Processors** details table, which displays the processor usage and simultaneous multithreading (SMT) usage and thread usage for each physical processor on the system.

System Assist Processors

Specifies displaying or hiding the **System Assist Processors** details table, which displays the processor usage for each System Assist Processor (SAP) on the system.

Logical Partitions

Specifies displaying or hiding the **Logical Partitions** details table, which displays the processor usage, processor type, and power consumption for each active logical partition on the system.

Channels

Specifies displaying or hiding the **Channels** details table, which displays the name of the owning logical partition or

```
Shared
```

if the channel is shared across partitions and the channel usage for each channel on the system.

Adapters

Specifies displaying or hiding the **Adapters** details table, which displays the channel assignment, adapter type, and usage for each Crypto and Flash adapter on the system.

Additional functions on this window include:

OK
To activate and save the current thresholds, click **OK**.

Reset
To reset the thresholds to the previously saved values, click **Reset**.

Cancel
To close the window without saving changes to thresholds, click **Cancel**.

Help
To display help for the current window, click **Help**.

Dashboard Histogram Display

Use this window to display this system activity data in histogram form. The system activity can be displayed in various intervals and durations dynamically. The usage(%), power (kW or Btu/hr), storage (kBytes/second), or temperature (°C or ºF) display on the left side of the histogram and the time intervals display on the bottom of the histogram.

Additional functions on this window include:

Clear
To clear the current histogram displayed and restart data collection, click **Clear**.

Pause
To pause the updating of the current histogram, click **Pause**.

Resume
To resume the updating of the current histogram, click **Resume**.

Export
To download the dashboard histogram data in a Comma Separated Values (CSV) file, click **Export**. This downloaded CSV file can then be imported into most spreadsheet applications.

Close
To exit this task, click **Close**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Frequency and Duration

Select the time frequency and duration for the system activity data to be displayed by using the down arrow on the entry field. The frequency and duration values are:

- 15 seconds for 1 hour
- 1 minute for 4 hours
- 5 minutes for 12 hours
- 10 minutes for 1 day

- 15 minutes for 2 days
- 1 hour for 10 days

Display Type

Select the type of system activity data to be displayed by using the down arrow on the entry field and selecting the desired data type. Depending on the targeted system details, the system activity display types can be one of the following:

System

- Processor Usage
- I/O Usage
- Power Consumption (kW)
- Power Consumption (Btu/hr)
- Ambient Temperature (ºC)
- Ambient Temperature (ºF)

Power Consumption

- Power Consumption (kW)
- Power Consumption (Btu/hr)
- Average Voltage
- Line current A
- Line Current B
- Line Current C

Input Air Temperature

- Input Air Temperature (ºC)
- Input Air Temperature (ºF)

Aggregated Processors

- All Processor Usage
- Shared Processor Usage

Processors

- Processor Usage
- Processor Usage by Key

System Assist Processors

- Processor Usage

Logical Partitions

- All Processor Usage
- CP Processor Usage
- IFL Processor Usage
- ICF Processor Usage
- zIIP Processor Usage

Channels

- Total Channel Usage

Adapters

- Total Adapters Usage

Set Thresholds

Use this window to set system activity thresholds for this system. A threshold value of 0 indicates no threshold is set. Depending on the type of threshold set, a warning indicator is displayed when the threshold value is reached. For processor and channel usage, the warning indicator is that the activity bar turns red. For power consumption and ambient temperature, the warning indicator is that the text turns red.

Thresholds are saved for the user ID.When you start the **Thresholds** task the current thresholds, if any were previously saved, are displayed. Otherwise, no thresholds are displayed.

Note: The default is no thresholds are set.

You can set threshold values for the following:

- Processor Usage (0 to 100%)
- Channel Usage (0 to 100%)
- Power Consumption (kW)
- Ambient Temperature (ºC)

Processors Usage
Specifies the threshold value, a percentage of 0-100 %, for the processor usage. After you specify the value, select the threshold type. An **Above** threshold displays a warning indicator when the processor usage value is above the threshold value. A **Below** threshold displays a warning indicator when the processor usage value is below the threshold value.

Channel Usage
Specifies the threshold value, a percentage of 0-100 %, for the processor usage. After you specify the value, select the threshold type. An **Above** threshold displays a warning indicator when the processor usage value is above the threshold value. A **Below** threshold displays a warning indicator when the processor usage value is below the threshold value.

Power Consumption
Specifies the threshold value, in kilowatts, for the power consumption. After you specify the value, select the threshold type. An **Above** threshold displays a warning indicator when the power consumption value is above the threshold value. A **Below** threshold displays a warning indicator when the power consumption value is below the threshold value.

Ambient Temperature
Specifies the threshold value, in degrees Celsius, for the ambient temperature. After you specify the value, select the threshold type. An **Above** threshold displays a warning indicator when the ambient temperature value is above the threshold value. A **Below** threshold displays a warning indicator when the ambient temperature value is below the threshold value.

Additional functions on this window include:

OK
To activate and save the current thresholds, click **OK**.

Reset
To reset the thresholds to the previously saved values, click **Reset**.

Cancel
To close the window without saving changes to thresholds, click **Cancel**.

Help
To display help for the current window, click **Help**.

Network Diagnostic Information

Accessing the Network Diagnostic Information task

This task displays network diagnostic information for the console's TCP/IP connection and allows you to send an echo request (ping) to a remote host.

To view information concerning the networking configuration on this Support Element console:

1. Open the **Network Diagnostic Information** task. The Network Diagnostic Information window is displayed.
2. Use the following tabs to view the network information:
   - Ping
   - Interfaces
   - Ethernet Settings
   - Address
   - Routes
   - Address Resolution Protocol (ARP)
   - Sockets
   - Transmission Control Protocol (TCP)
   - Internet Protocol (IP) Tables
   - User Datagram Protocol (UDP)
   - DNS
   - Native Connections
3. Click **Cancel** when you are done viewing the information.

Network Diagnostic Information

You can use the console workplace to obtain network diagnostic information about the Support Element's network protocols. Use this window to access any one of the following *Network Diagnostic Information* tabs:

- Ping
- Interfaces
- Ethernet Settings
- Address
- Routes
- ARP (Address Resolution Protocol)
- Sockets
- TCP (Transmission Control Protocol)
- IP (Internet Protocol) Tables
- UDP (User Datagram Protocol)
- DNS
- Native Connections

Cancel
To close this window and cancel the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Ping

Use this page to send an echo request (ping) to a remote host to see if the host is accessible and to receive information about that TCP/IP address or name.

TCP/IP Address or Name to Ping
Specify any TCP/IP address or host name in this field, then click **Ping**. The results for that TCP/IP address or host name are displayed in the page.

Ping
To send a ping command for the TCP/IP address or host name you specified in the field, click **Ping**.

Interfaces

Use this page to display the statistics for the network interfaces currently configured. To update the information that is currently displayed with the most recent information, click **Refresh**.

Ethernet Settings

Use this page to display the settings for the ethernet cards currently configured. To update the information that is currently displayed with the most recent information, click **Refresh**.

Address

Use this page to display TCP/IP addresses for the configured network interfaces. To update the information that is currently displayed with the most recent information, click **Refresh**.

Routes

Use this page to display the Kernel IP and IPv6 routing tables and corresponding network interfaces. To update the information that is currently displayed with the most recent information, click **Refresh**.

ARP

Use this page to display the contents of the Address Resolution Protocol (ARP) connections. To update the information that is currently displayed with the most recent information, click **Refresh**.

Sockets

Use this page to display information about TCP/IP sockets. To update the information that is currently displayed with the most recent information, click **Refresh**.

TCP

Use this page to display information about Transmission Control Protocol (TCP) connections. To update the information that is currently displayed with the most recent information, click **Refresh**.

IP Tables

Use this page to display information (in table format) about the Internet Protocol (IP) packet filter rules. To update the information that is currently displayed with the most recent information, click **Refresh**.

UDP

Use this page to display information about User Datagram Protocol (UDP) statistics. To update the information that is currently displayed with the most recent information, click **Refresh**.

DNS

Use this page to verify a Domain Name Services (DNS) server.

TCP/IP Address to Resolve
Specify a TCP/IP address in this input field, then click **DNS**.

DNS
To provide detailed information for the specified TCP/IP address to resolve, click **DNS**.

Native Connections

Use this page to display all of the native TCP/IP base communication service connections. To update the information that is currently displayed with the most recent information, click **Refresh**.

Network Traffic Analyzer Authorization

Accessing the Network Traffic Analyzer Authorization task

Use this task for the selected OSA-Express or HiperSockets channel to customize or check the current authorization to trace network traffic. This task allows you to select:

- Customize network traffic analyzer settings
- Check current network traffic analyzer authorization.

To customize or check the network traffic analyzer settings:

1. Locate the **CPC** to work with.
2. Locate the OSA-Express or HiperSockets **Channel** you want to work with.
3. Open the **Network Traffic Analyzer Authorization** task.
   - For OSA-Express, the Network Traffic Analyzer Controls window displays.
   - For HiperSockets, the HiperSockets Network Traffic Analyzer Authorization window displays.
4. Depending on the channel type you have selected:
   - For OSA-Express, select the appropriate control task to:
     - *Customize Network Traffic Analyzer Settings...* to set up NTA authorization to allow or disallow the OSA channels from tracing outside of their own partition.
     - *Check current Network Traffic Analyzer authorization...* to allow the Support Element to scan all the OSA channels and report back which OSA channels are authorized for NTA to trace outside its own partition.
   - For HiperSockets, select the network traffic analyzer logical partition and eligible logical partitions that will be authorized to set up, trace, and capture the HiperSockets network traffic.
     - All IQD channels are not authorized to enable HiperSockets NTA
     - This IQD channel is not authorized to enable HiperSockets NTA
     - This IQD channel is authorized to enable, control and capture network traffic from all logical partitions that contain the IQD CHPID that maps to this IQD channel (Caution: This setting will result in tracing all traffic flowing between all the logical partitions using this IQD CHPID. This can result in performance degradation)
     - Customized HiperSockets NTA logical partition authorization list for this IQD channel.
5. Click **OK** to perform the selected operation.

Network Traffic Analyzer Controls

Use this window to select a Network Traffic Analyzer (NTA) control to enable or check the current authorization to trace network traffic. The following selections are available:

- Customize Network Traffic Analyzer Settings...
- Check current Network Traffic Analyzer Authorization...

OK
To continue with the operation, click **OK**.

Cancel
To close the window without saving changes you made, click **Cancel**.

Help
To display help for the current window, click **Help**.

Current Network Traffic Analyzer Authorization

This window displays the current channels that are authorized for the Network Traffic Analyzer to trace outside their own logical partitions.

OK
To close the window and return to the previous window, click **OK**.

Disable the Host Network Traffic Analyzer from tracing outside of the channel's own partition
To disable a channel authorized from the Network Traffic Analyzer tracing outside of the logical partition, select the channel from the above list then select **Disable the Host Network Traffic Analyzer from tracing outside of the channel's own partition**.

Help
To display help for the current window, click **Help**.

OSA-Express Host Network Traffic Analyzer Authorization

Use this window to select the level of authorization for the OSA-Express host network traffic analyzer. The Channel ID, type, and card description are displayed.

Status
You can use the Status table to check or change the single or multi-port network traffic analyzer authorization definitions for the selected channel. Select from the following choices the level of authorization you want for the OSA-Express Host Network Traffic Analyzer.

- Logical Partition - tracing allowed for resources define within the tracing host logical partition (this is the default)
- CHPID - Displays for a single port that allows tracing for all resources defined to this CHPID for all logical partitions sharing this CHPID
- Port - Displays for a multi-port that allows tracing for all resources defined to this port and for all logical partitions sharing this port
- Disabled - All tracing by the Host Network Traffic Analyzer is disallowed.

OK
To apply the changes you made, click **OK**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Customize a HiperSockets NTA logical partition authorization List

Use this window to select the NTA logical partitions and eligible logical partitions that will be authorized to setup, trace, and capture the HiperSockets network traffic. To define NTA rules for each logical partition perform the following:

To authorize an NTA logical partition:

1. Click the NTA logical partition that will be authorized to set up, trace, and capture the HiperSockets network traffic.
2. Select the eligible logical partitions to be traced; you are required to select at least one eligible logical partition for authorization.

Only traffic flowing between the selected eligible logical partition or logical partitions is traced.

To remove authorization from a logical partition:

1. Click the NTA logical partition that is currently authorized.
2. Clear all eligible logical partitions.

Repeat the appropriate series of steps for all logical partitions for which the NTA rules need updating. Click **OK** to accept the changes.

OK
To apply the changes you made, click **OK**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

HiperSockets Network Traffic Analyzer Authorization

Use this window to select the level of authorization for the HiperSockets NTA Logical Partition. The Channel ID, type, and card description are displayed. Select from the following choices the level of authorization you want for the HiperSockets NTA logical partition:

- All IQD channels are not authorized to enable HiperSockets NTA
- This IQD channel is not authorized to enable HiperSockets NTA
- This IQD channel is authorized to enable, control and capture network traffic from all logical partitions that contain the IQD CHPID that maps to this IQD channel
- Customized HiperSockets NTA logical partition authorization list for this IQD channel.

Submit
To apply modified NTA rules for the selected HiperSocket channel, select **Submit**.

Change Customized Settings...
To customize what partitions will be NTA authorized to trace and what partitions are eligible to be traced, select **Change Customized Settings...**.

Save Current Settings
To save and backup the current NTA authorization rules for all the HiperSocket channels, select **Save Current Settings**. Use this to save your current rules while you make a temporary change, then you can restore them later.

Restore Saved Settings
To restore the previous saved NTA authorization rules for all the HiperSocket channels, select **Restore Saved Settings**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Nondisruptive Hardware Change

Nondisruptive Hardware Change

Use this window to confirm or cancel your request to start a procedure that will provide instructions for changing the hardware configuration of a machine while it is powered-on and operating.

Follow the procedure to install cards on the central processor complex (CPC) and its expansion cage(s).

Additional functions on this window include:

Install
To verify CPC power is on, and to start the installation procedure, click **Install**.

Note: Whether or not the CPC is operating, its power must be on to use the card installation procedure.

Remove
To verify CPC power is on, and to start the removal procedure, click **Remove**.

Note: Whether or not the CPC is operating, its power must be on to use the card removal procedure.

Cancel
To close this window without starting the installation or removal procedure, click **Cancel**.

Help
To display help for the current window, click **Help**.

Nondisruptive Hardware Change - Install

Use this window to select the type of hardware to install on the central processor complex (CPC) or its expansion cage(s).

Use the hardware description list to select one type of hardware to install, then click **OK**.

The hardware description list displays the types of cards that are supported by the machine type and model of the CPC.

Additional functions on this window include:

OK
To view the card slots available for installing the selected type of hardware and continue the procedure for installing the hardware, click **OK**.

Cancel
To close this window without continuing the hardware install, click **Cancel**.

Help
To display help for the current window, click **Help**.

Nondisruptive Hardware Change - Available Locations

Use this window to select the card locations to plug the selected hardware.

Select from the list the locations to plug the selected hardware.

Additional functions on this window include:

OK
To continue the procedure for installing the hardware in the selected locations, click **OK**.

Cancel
To close this window without continuing the hardware install, click **Cancel**.

Help
To display help for the current window, click **Help**.

Nondisruptive Hardware Change - Port Locations

This window identifies the port locations where cables need to be plugged on the cards just installed.

Additional functions on this window include:

OK
To finish the install procedure after the cables have been plugged, click **OK**.

Help
To display help for the current window, click **Help**.

Nondisruptive Hardware Change - Removal Options

Use this window to choose the type of hardware to remove.

Additional functions on this window include:

Remove hardware

To view the locations available for removal of the selected hardware type(s), click **Remove hardware**.

Cancel
To close this window without continuing the hardware install, click **Cancel**.

Help
To display help for the current window, click **Help**.

Nondisruptive Hardware Change - Remove Locations

Use this window to select the locations to remove the selected hardware.

Select from the list the FRU locations to remove the hardware.

Select from the list of STI locations to remove the hardware.

Note: If a location displays on the window that you did not select previously, you may have plugged it into the wrong location. Verify you plugged the FRU into the right slot.

Additional functions on this window include:

Continue
To continue the procedure for removing the hardware from the selected locations, click **Continue**.

Cancel
To close the window and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Nondisruptive Hardware Change - Remove Locations Confirmation

This window identifies the locations to remove the selected hardware.

This list identifies the FRU locations prepared for removal.

This list identifies the STI locations prepared for removal.

Additional functions on this window include:

Continue
To continue the procedure for removing the hardware from the selected locations, click **Continue**.

Cancel
To close the window and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Nondisruptive Hardware Change - LICCC Enablement

This window identifies what cards require LICCC data.

Displays the location and serial number of the cards that require LICCC data.

Additional functions on this window include:

Continue
To continue with the LICCC Enablement install, click **Continue**.

Continue without LICCC data
To continue without the LICCC Enablement, and to enable LICCC at a later time, click **Continue without LICCC data**.

Help
To display help for the current window, click **Help**.

PCHIDs not in Service Mode

This window identifies what PCHIDs are not in Service Mode. All the PCHIDs associated with the cards being removed must be in Service Mode to continue with the removal.

The list of PCHIDs that need to be placed in Service Mode.

Additional functions on this window include:

OK
Once the listed PCHIDs have been put in Service Mode, click **OK**.

Cancel
To close the window and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

CHPIDs not Offline

This window identifies what CHPIDs are not Offline. All the CHPIDs associated with the cards being removed must be offline to continue with the removal.

The list of CHPIDs that need to be turned Offline from the console.

Additional functions on this window include:

OK
Once the listed CHPIDs have been turned Offline, click **OK**.

Cancel
To close the window and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Crypto Assignment

Use this window to reassign Cryptos for the cards plugged.

This identifies the current Crypto value for the listed location.

Note: An '*' indicates that this Crypto was a previous assignment for this card.

Additional functions on this window include:

OK
When you have completed reassigning the Cryptos, click **OK**.

Show defaults
To reset the panel with the original Crypto assignments, click **Show defaults**.

Help
To display help for the current window, click **Help**.

Nondisruptive Hardware Change - Install Locations Confirmation

This window identifies the locations to install the selected hardware.

This list identifies the locations to plug the selected hardware.

Note: If a location displays on the window that you did not select previously, you may have plugged it into the wrong location. Verify you plugged the FRU into the right slot.

Additional functions on this window include:

Configure
To continue the procedure for configuring the hardware after it has been installed, click **Configure**.

Cancel
To close this window without continuing the hardware install, click **Cancel**.

Help
To display help for the current window, click **Help**.

Nondisruptive Hardware Change - Card Slot Location

The card slot location identifies the location of a card slot in a frame and the type of card you can install in it.

Card slots are located in the card section of a central processor complex (CPC) or an expansion cage.

A card slot location is identified by eight characters. The first character identifies the location of its frame in the machine.

A
Identifies the right most frame.

Z, Y, X, W, or V
Identify frames attached to the left of frame A.

The next three characters identify the location of the CPC or expansion cage within the frame.

01B
Indicates the location is the bottom of the frame.

19B
Indicates the location is the top of the frame.

The next two characters identify the type of card you can install in the slot.

D1
Identifies any half cards or MBA cards. It indicates that this is the top slot of a mother card or the first MBA location in a Book.

D2
Identifies any half cards or MBA cards. It indicates that this is the bottom slot of a mother card or the second MBA location in a Book.

D3 thru D8
Identifies an MBA card. It indicates that this is the third thru eigth MBA location in a Book.

LG
Identifies a logic card

The last two characters are for the two-digit decimal number assigned to the card slot in the CPC or expansion cage. Half of the card slots in a CPC or expansion cage face the front of the frame, the other card slots face the rear of the frame.

01 thru 13
Indicate the card slot faces the front of the frame. As you face the card slots, they are numbered from left to right.

14 thru 26
Indicate the card slot faces the rear of the frame. As you face the card slots, they are numbered from left to right.

Nondisruptive Hardware Change - List Selection

To select one or more items from a listbox, refer to the following rules:

- To select one location from the remove list, click the left mouse button on that location.
- To select multiple non-consecutive locations from the remove list, position the cursor over the list, then hold down the **Ctrl** key and click the left mouse button once on all desired locations.
- To select multiple consecutive locations from the remove list, click the left mouse button on the first desired location. Then, position the cursor over the last desired location in the list, hold down the **Shift** key, and click the left mouse button to highlight all the locations between the first and last location selected.

Object Locking Settings

Accessing the Object Locking Settings task

This task allows you to control whether managed objects are automatically locked and whether they are re-locked after being used as target objects for a task.

To lock or unlock objects:

1. Open the **Object Locking Settings** task. The Locking window is displayed.
2. Select the setting you want set for the object.
3. Click **OK** to proceed or **Cancel** to exit the task without changing the setting.

Locking

You can control whether managed objects are to be automatically locked after changes to this window are applied or they are locked automatically after used as target objects for a task. Changes apply only to objects that support lockout disruptive tasks

Customize the settings to indicate your preferences, then click **OK**.

Automatically lock all managed objects
To control whether or not managed objects should be automatically locked after they are used as target objects for a task, select **Automatically lock all managed objects**.

- If this is not selected (no check mark appears), the managed objects are not to be automatically locked after they are used as target objects for a task.
- If this is selected (a check mark appears), the managed objects that support lockout disruptive tasks are to be automatically locked when the changes to this window are applied. In addition, all managed objects are to be locked when the console is started and an object is automatically locked when created.

Relock after a task has been run
To relock the managed objects after a task has been run, select **Relock after a task has been run**.

OK
To customize the settings to your selected preferences, click **OK**.

Reset
To discard any changes you made to the settings in this window and to re-display the current settings for this window, click **Reset**.

Defaults
To return to the object locking settings that are the default for the current user, click **Defaults**.

Cancel
To exit this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Offload Problem Analysis Data to Removable Media

Accessing the Offload Problem Analysis Data to HMC Removable Media task

This task allows you to copy problem data onto a hardware management console removable media when there is no external connections for your Hardware Management Console to send problem data.

To offload problem analysis data to the HMC Removable Media:

1. Open the **Offload Problem Analysis Data to HMC Removable Media** task.

   The Problem Analysis Data Offload window displays.
2. Select the *problem number* of the subdirectory you want to offload from the list
3. Insert the removable media in the Hardware Management Console that is formatted with a volume label of: VIRTRET.
4. Click **OK** to initiate the offload.

   This offload process takes several minutes, depending on the size and quantity of the files to be transferred to removable media.

Offload Problem Analysis Data to Removable Media

Problem analysis is a set of subdirectories that contain all the files that would have been transmitted to the support system if a connection to the support system were available. A subdirectory is dynamically created for each problem reported on a machine that was unable to send data to the support system. You can offload the data for a given problem within one of these subdirectories directly to removable media on the Hardware Management Console.

The label of each subdirectory represents a problem number.

Data is offloaded to removable media on the Hardware Management Console using the Single Object Operations direct connection to the Support Element. To establish a Support Element session from the Hardware Management Console:

1. Select the Support Element that you want to connect to.
2. Open **Single Object Operations** from the **Recovery** task list. The **Single Object Operations Task Confirmation** window is displayed.
3. If you want to continue establishing a session, click **Yes**.

From the **Service** task list on the Support Element, select **Offload Problem Analysis Data to Removable Media** task icon to initiate the window. The window allows you to choose the problem number for the data you want to write to the removable media on the Hardware Management Console.

Use this window to choose which problem data to offload to removable media. Load a removable media which is formatted with no volume label or a volume label of VIRTRET into the removable media drive. Select the problem number from the list in the window; then, click **OK** to begin the offload.

The offload process takes several minutes to complete, depending on the size and quantity of the files to be transferred to removable media.

After the offload process is started, a busy dialog is displayed while the process is in progress. After the process has completed, a message window is displayed indicating that the offload was completed successfully or that an error was encountered during the offload.

Possible error messages include:

- Error transmitting data to the Hardware Management Console.
- Media does not have enough space for file offload.
- Format removable media with VIRTRET as volume label.
- There is no problem analysis data to offload.
- Error mounting, media not inserted...
- Error mounting, unrecognized file system... possibly unformatted media.
- This task must be performed from a Hardware Management Console.

Note: When you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message is displayed indicating the drive was not added and that you should remove the device and try again

Problem number
A problem number corresponds to the label of each subdirectory. Select a problem number in the list to select the problem data to offload to the removable media.

OK
To begin the offload for the problem number you selected, click **OK**.

Cancel
To close the window without performing the offload, click **Cancel**.

Help
To display help for the current window, click **Help**.

Operating System Messages

Accessing Operating System Messages

Displays consolidated operating system generated messages for all selected images. These messages are available to all default user IDs.

An image is a set of central processor complex (CPC) resources capable of running a control program or operating system. An operating system running in an image sends messages to operating system consoles to notify you of significant events that involve or affect the use of the operating system. The messages are referred to as *operating system messages*.

If an operating system running in an image supports console integration and is customized to allow using the console as an operating system console, then the console can also receive operating system messages.

An operating system may issue any number of messages at any time. The console receives the messages automatically and stores them in a message log. The console also turns on several console indicators to help you recognize that priority or held operating system messages were received. A *priority* or held operating system message either requires a response from the console operator or notifies the console operator of a critical condition that requires immediate attention.

The console can store an average of approximately 200 (depending on the length of each message) messages in its operating system message log per image. If the message log becomes full, the console continues to receive and store new messages, but deletes one or more of the log's oldest non-held, non-priority messages to make room for each new message. If there are not any non-held, non-priority messages, the oldest non-held priority, held, or priority message will be deleted.

Note: Depending on your user task role, you may only be able to view the operating system messages.

To display the **Operating System Messages:**

1. Select the desired CPC or images.
2. Open the **Operating System Messages** task.
3. The Operating System Messages window opens.
4. Select the operation you want to perform from the Operating system Messages.

Operating System Messages

If operating systems running in one or more Central Processor Complex (CPC) images support console integration and are customized to allow by using the console as an operating system console, then use **Operating System Messages** to:

- Display, manage, and respond to operating system messages from the CPC images.
- Send operating system commands to the CPC images.

Note: This task may be view only for some user task roles.

Console integration is a facility of the console. An operating system that supports console integration can be customized to allow by using the console, if necessary, as an operating system console.

Under normal conditions, while other operating system consoles are available, the console should *not* be used as an operating system console. That is, the console integration facility is not intended to make the console the primary user interface to an operating system.

The console integration facility is intended instead to allow by using the console as an operating system console only when other operating system consoles are not available. For example, other operating system consoles are not available:

- During initialization of the operating system
- During outages or failures

- For Coupling Facility Control Code (CFCC).

This window displays and manages messages that are issued by operating systems running images managed by this console.

System
Select the operating system running image from the drop-down list to display system their messages.

Toolbar
Click the toolbar icons or **Actions** drop-down arrow to perform the following:

Respond 
Enter a response to the selected message from the partition list you want to send a message, then click **Send**. You can also right-click on the message from the list, and then click **Respond**.

If the operating system sent a default response for the selected message, then the default response displays in this field. Otherwise, you can specify any other response, up to 200 characters.

Note: The **Respond** icon does not display if the current operating system does not support the **Respond** function.

Delete 
Delete selected messages for the partition list, then click **Yes**. You can also right-click on the message from the list, and then click **Delete**

Export 
Select from the drop-down arrow to **Export as HTML** or **Export All to CSV** messages for the selected running system image.

Note: The **Export** and **Print** options are available remotely only.

Print 
Select from the drop-down arrow to **Print All** messages, **Print Selected** messages, or **Print Preview** display of messages for the selected running system image.

Note: The **Export** and **Print** options are available remotely only.

Actions
Select from the drop-down arrow to **Delete** or **Respond** to a message for the selected running system image.

Note: The **Export** and **Print** actions are available remotely only.

Filter

Use the Filter function to enter a filter string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

Message
Displays operating system messages for the current selected image and any message that was received.

Command
Enter a command message to send to the operating system, then click **Send**.

Priority message
Sends message commands with greater importance when checked.

Note: Some systems do not accept priority messages.

Close
To close the current window, click **Close**.

Help
To display help for the current window, click **Help**.

Viewing operating system messages

View operating system messages to remain informed of events that involve or affect the use of images supported by the central processor complex (CPC). Upon viewing operating system messages, you can also:

- Send responses to messages.
- Delete messages you no longer need.
- Use the online Help for more information to view, respond to, or delete operating system messages.

To view operating system messages:

Black
Indicates an informational message that normally does not require a response from the console operator.

Blue
Indicates a held message that requires a response from the console operator.

Red
Indicates a priority message about a critical condition that requires immediate attention.

Responding to an operating system message requires receiving an operating system message first. You can use **Operating System Messages** also to send commands to an operating system, regardless of whether you've received messages from it.

Sending commands to the operating system

You can use the console to send commands, at any time, to operating systems running in images supported by the central processor complex (CPC).

To send commands to an operating system:

1. Locate a target: either a group of images or individual images. Using a group of images allows sending commands to each operating system running on images in the group, while using individual images allows sending commands to their operating systems only.
2. Locate and open the **Operating System Messages** task.

   This opens the Operating System Messages window. The window lists the operating system messages, if any, from each image in the target group or among the selected images.
3. If the current operating system supports priority messages, a priority checkbox displays on the window. Select the checkbox to send a priority message.
4. Enter a command in the **Command** field.
5. Click **Send** to send the command to the operating system running on the images.

   Note: The **Priority** checkbox is not available if the operating system running on an image does not support receiving priority commands from the console.

Related information

- Refer to the publications provided with your operating system for more information about whether it supports console integration, and how to customize it to allow using the console as an operating system console.

Partition Details

Accessing the Partition Details task

Use the **Partition Details** task to view or modify an existing definition for a specific partition. You can access this task from the main HMC page by selecting a partition under a specific Dynamic Partition Manager (DPM)-enabled system in the Systems Management node, or by selecting the task in the Tasks index.

Note: This task is available on the HMC only when one or more managed systems have DPM enabled.

To open the **Partition Details** task, you must have a customized user ID either with authorization to the task, or with one of the following predefined roles: System Programmer Tasks or Service Representative Tasks. You also can use the default SERVICE user ID, but using a customized user ID is the suggested practice.

The **Partition Details** task is also available on the Support Element (SE) in view-only mode.

To modify a partition definition:

1. On the HMC, select a DPM-enabled system in the Systems Management node.
2. On the Partitions tab, click the hyperlink in the Name column for a specific partition. The Partition Details window opens.
3. Review and, if necessary, modify values in the **General**, **Status**, **Controls**, **Processors**, **Memory**, **Network**, **Storage**, **Cryptos**, and **Boot** sections. Note that the **Partition links** page only provides links for more information, because a partition link can be attached to existing partitions only. To attach a partition link to one or more existing partitions, use the **Configure Partition Links** task. To access each section, click the link in the navigation frame, or scroll and use the expand and collapse buttons in the section headings, as necessary.

   Note: To access the **Controls** section, you must be using the default SERVICE user ID, or a customized user ID with either the System Programmer Tasks role or the Service Representative Tasks role. If you are not logged on with a user ID that has the required authority, the **Controls** section is not displayed.
4. When you have finished, click **OK** to save your changes. If you made changes to a partition that is not in Stopped state, a confirmation window opens. Click **Save** to save your changes. A progress indicator is displayed until DPM finishes the updating the partition.

When it has completed the operation, DPM opens the Validation window, which indicates whether the partition was successfully updated.

- If the save operation did not complete successfully, the Validation window displays an error message with details about the problem. In this case, click **Close** to return to the **Partition Details** task. Depending on the error, the task opens to either the main window or the first section, if any, that contains an error.
- If you have created one or more network interface cards (NICs) with associated VLAN IDs, the Validation window includes a list of each NIC device number and the associated VLAN ID to be used when configuring the device on the operating system that the partition hosts.

Partition Details

Use the **Partition Details** task to view or modify an existing definition for a specific partition on a Dynamic Partition Manager (DPM)-enabled system.

To open the **Partition Details** task, you must have a customized user ID either with authorization to the task, or with one of the following predefined roles: System Programmer Tasks or Service Representative Tasks. You also can use the default SERVICE user ID, but using a customized user ID is the suggested practice.

The **Partition Details** task opens in view-only mode under the following circumstances:

- When you access the task from the Support Element (SE), rather than the Hardware Management Console (HMC).
- When the current status of the DPM-enabled system is one of the following: No power, Not operating, Service, Status check, or Communications not active.

The **Partition Details** task is organized into the following sections, each of which are listed in the navigation pane. To access each section, click the appropriate link in the navigation pane, or scroll the main page and expand or collapse each section as necessary.

- "General" on page 696
- "Status" on page 698
- "Controls" on page 699
- "Processors" on page 700
- "Memory" on page 703
- "Network" on page 705
- "Storage" on page 711
- "Cryptos" on page 720
- "Partition links" on page 727
- "Boot" on page 728

The navigation pane also includes the following links to related tasks.

Start or Stop
Depending on the current status of the selected partition, only one of the following task links is displayed.

Start
Opens the **Start** task, with this partition selected as the partition to start.

Stop
Opens the **Stop** task, with this partition selected as the partition to stop.

System Details
Opens the **System Details** task for the DPM-enabled system.

Manage Adapters
Opens the **Manage Adapters** task for the DPM-enabled system.

Monitor System
Switches the foreground window to the **Monitor** tab for the selected DPM system node.

You can find more detailed help on the following elements of this window:

OK
To close the window, click **OK**. This action applies your changes and closes the Partition Details window.

- If you made changes to a partition that is not in Stopped state, a confirmation window opens. Click **Save** to save your changes or **Cancel** to close the window without saving any of your changes. If you click **Save**, a progress indicator is displayed until DPM finishes the updating the partition.
- If you made changes to a partition that is in Stopped state and click **OK**, a progress indicator is displayed until DPM finishes the updating the partition.

When it has completed the operation, DPM opens the Validation window, which indicates whether the partition was successfully updated. If not, the Validation window displays an error message with details about the problem. In this case, click **Close** to return to the **Partition Details** task. Depending on the error, the task opens to either the main window or the first section that contains an error.

Apply
To apply changes you made in editable fields on the page, click **Apply**. This action applies your changes without closing the Partition Details window.

- If you made changes to a partition that is not in Stopped state, a confirmation window opens. Click **Save** to apply the changes or **Cancel** to return to the previous window. If you click **Save**, a progress indicator is displayed until DPM finishes the updating the partition.
- If you made changes to a partition that is in Stopped state, a progress indicator is displayed until DPM finishes the updating the partition.

When it has completed the operation, DPM opens the Validation window, which indicates whether the partition was successfully updated. If not, the Validation window displays an error message with details about the problem. In this case, click **Close** to return to the **Partition Details** task. Depending on the error, the task opens to either the main window or the first section that contains an error.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Help
To display help for the current window, click **Help**.

In view-only mode, only **Cancel** and **Help** are displayed.

General

Use the General section to view or modify the general details for this partition.

On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Name
Specifies the name of the partition, which can be 1 - 64 characters in length. Supported characters are alphanumerics, blanks, periods, underscores, dashes, or at symbols (@). Names cannot start or end with blank characters. A partition name must uniquely identify the partition from all other partitions defined on the same system.

Description
Specifies the user-supplied description, if any, of the partition. The description can be up to 1024 characters in length.

Object ID
Displays the DPM-generated identifier for this partition. This ID is also known as the universally unique identifier (UUID) of the partition.

Mode
Displays the operating mode of the hypervisor or operating system on the partition.

Short name
Specifies the short name of the partition, which is the name by which the operating system can identify the partition. The short name must consist of 1 - 8 alphanumeric uppercase characters, with the first character is alphabetic; the words PHYSICAL, REC, SYSTEM, and PRIMxxxx (where xxxx is a 4-digit decimal number) are reserved and cannot be used.

- If the short name that you provide has been specified for another partition, the name is valid only if you are not reserving resources for this partition. The best practice, however, is to supply a unique name that identifies the partition from all other partitions defined on the same system. An error or warning message is displayed if the short name is not unique.
- If you delete the value specified for this field, a unique short name is automatically generated when you save your changes.

Partition ID
Specifies the identifier (ID) for the partition. Select **Generate automatically** to allow the partition ID to be managed by the system; by default, this check box is selected. When **Generate automatically** is selected, the partition has a different ID each time it is started.

The partition ID must be a unique two-character hex number from 00 - 7F. If the partition ID that you provide has been specified for another partition, the ID is valid only if you are not reserving resources for this partition. Even in this case, however, the best practice is to supply a unique ID.

Partition type
Specifies one of the following values that identifies the type of partition. You cannot change the partition type.

Linux
In this type of partition, you can install and run a Linux distribution as a single operating system, or as a hypervisor for multiple guests.

z/VM
In this type of partition, you can install and run z/VM as a hypervisor for multiple Linux guests.

Secure Service Container
This type of partition is a Secure Service Container, in which you can run only specific software appliances that the Secure Service Container supports.

When the selected partition type is **Secure Service Container**, the page display includes the following additional fields. These fields are read-only until you click **RESET LOGIN**.

Master User ID
Enter the user ID to be used as the default master user ID for the Secure Service Container partition. This user ID has authority to perform any task that is available through the Secure Service Container graphical user interface (GUI).

A master user ID can be 1 - 32 characters long. It cannot contain blanks. Valid characters are numbers 0 - 9, letters A - Z (upper or lower case), and the following special characters: period (.), underscore (_), and hyphen (-).

Master Password
Enter the password for the master user ID. A master password can have a minimum of 8 characters and a maximum of 256 characters. A master password is case-sensitive and can contain numbers 0 - 9, letters A - Z (upper or lower case), and the following special characters: hyphen (-), underscore (_), exclamation (!), at (@), hash (#), dollar ($), percent (%), carat (^), ampersand (&), asterisk (*), left parenthesis (), right parenthesis ()), plus (+), left brace ({), right brace (}), vertical bar (|), colon (:), less than (<), greater than (>), question mark (?), and equals (=).

Confirm Master Password
Reenter the password exactly as you typed it for the Master Password field.

RESET LOGIN
Click **RESET LOGIN** to remove any previously supplied password and confirmation from the password text fields, so you can supply new values for **Master User ID**, **Master Password**, and **Confirm Master Password**. To save these new values, click **Apply**; to have the saved values take effect, you must stop and restart the partition. Otherwise, click **Cancel** to cancel the reset operation.

Reserve resources to ensure they are available when the partition is started
Specifies whether or not resources are reserved for this partition. Select this check box only if you want to reserve the configured resources for this partition, which include processors, memory, network interface cards, host bus adapters, virtual functions, and crypto domains.

- When this check box is not selected, other partitions on the system can use these resources when this partition is stopped. In this case, this partition might be unable to start if the required resources are not available.
- When this check box is selected, these resources cannot be used by any other partition on the system, even when this partition is stopped. This selection guarantees that the partition can be started at any point in time.

OS name
Displays the user-defined name of the hypervisor or operating system for this partition. The value for this field is displayed only when DPM has detected the hypervisor or operating system.

OS type and level
Displays the type and release level of the hypervisor or operating system that is running on this partition; for example: Linux 3.11.0. The value for this field is displayed only when DPM has detected the hypervisor or operating system.

Secure Execution
Indicates whether the operating system that runs on the partition is configured for secure execution, which isolates and protects any guests that run on a hypervisor by restricting host access to guest workloads and data.

On
This field value is displayed only when the operating system is configured for secure execution and is running, and the partition is active.

Off
This field value is displayed when one of the following conditions is true.

- The IBM Secure Execution for Linux feature is not enabled on the host system for this partition. In this case, the field value does not change to On, even if the operating system is configured for secure execution.
- The operating system is not configured for secure execution.
- The operating system is configured for secure execution but the partition is not active.

Status

Use the Status section to view the current status of the partition and, if necessary, to modify the acceptable availability status values for the partition, based on the importance of its workload. For example, if this partition supports a critical workload on a production server, you might select only Active as an acceptable status value. In contrast, for a partition that supports low-priority software testing, you might select additional values as acceptable. When a partition is started and enters a state that is not selected as an acceptable status, the partition is highlighted in red in various HMC task displays.

In this section, the Status field displays the current status of the partition. The current status value is preceded by an icon that indicates whether this current status value is defined as an acceptable status value. If the current status value is Degraded, the display includes a message indicating the reason why the status is Degraded, and lists the name of each resource that is causing the partition to be in the Degraded state. Each list item is a hyperlink through which you can open the details window for the resource. When one or more storage adapters are degraded, the list includes affected storage groups or tape links, along with a hyperlink to the appropriate storage group or tape link details page.

Under the "Acceptable statuses" label, you can select one or more status values as an acceptable status for the partition. When you have finished, review another section or click **OK** to save the partition definition.

By default, only Active is selected.

Active
Indicates that the partition has successfully started and is operating normally.

Communications not active
Indicates a problem with the communication between the Hardware Management Console (HMC) and the Support Element (SE).

Degraded
Indicates that the partition successfully started and is operating, but the availability of physical resources to which it has access is less than required, as stated in the partition definition. This status might be acceptable, for example, for partitions that do not have reserved resources.

Paused
Indicates that, because a user has stopped all processors, the partition is not running its workload. In this case, because the partition was successfully started, its resources are shown as active and are still associated with this partition.

Reservation error
Indicates that the availability of physical resources does not match the reserved resources that are stated in the definition for this partition. The partition cannot start until sufficient resources are available.

Starting
Indicates the transitional phase between Stopped state and Active state, as the result of a Start task issued against this partition.

Status check
Indicates that the current status of the partition is unknown. This condition usually occurs under one of the following circumstances:

- When the SE is starting up; in this case, this partition status is temporary.
- When the SE and the DPM-enabled system to which it is attached cannot communicate.

Stopped
Indicates that the partition has normally ended its operation, and exists only as a partition definition.

Stopping
Indicates the transitional phase between Active state and Stopped state, as the result of a Stop task issued against this partition.

Terminated
Indicates that all of the processors for this partition are in a disabled wait state, or a system check stop occurred. The partition is not running its workload. In this case, because the partition was successfully started, its resources are shown as active and are still associated with this partition.

Controls

Use the Controls section to enable or disable partition access to various controls. By default, all settings are unchecked.

Note: To access the **Controls** section, you must be using the default SERVICE user ID, or a customized user ID with either the System Programmer Tasks role or the Service Representative Tasks role. If you are not logged on with a user ID that has the required authority, the **Controls** section is not displayed.

Partition Access Controls
You can select one or more of the following security-related controls.

Access global performance data
Select this option:

- To allow the partition to view the CPU utilization data and the Input/Output Processor (IOP) data for all partitions in the configuration. If you do not select this option, the partition is only able to view its own CPU utilization data.
- To enable the collection of FICON channel measurements.

Permit cross-partition commands
Select this option to allow the partition to issue control program commands that affect other partitions; for example, perform a system reset of another partition, deactivate a partition, or provide support for the automatic reconfiguration facility.

CPU-Measurement Counter Facility Authorization Controls
The CPU-measurement counter facility provides a means to measure activities in the CPU and some shared peripheral processors. Select these options only when you want to collect measurement data for performance statistics.

Access basic counter set
Select this option to authorize the use of the basic counter set. This set includes counts of central processing unit cycles, instructions executed, and directory-write and penalty cycles for level-1 instruction and data caches.

Access problem state counter set
Select this option to authorize the use of the problem state counter set. This set includes counts of central processing unit cycles, instructions executed, and directory-write and penalty cycles for level-1 instruction and data caches only when the processor is in problem state.

Access crypto activity counter set
Select this option to authorize the use of the crypto activity counter set. This set includes counters for a central processing unit that are related to the following function counts.

- Pseudo Random Number Generation (PRNG)
- Secure Hash Algorithm (SHA)
- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

Access extended counter set
Select this option to authorize the use of the extended counter set. The extended counters provide information about hardware facilities and structures that are specific to a machine family. The extended counters are designed to expand upon information provided by the basic counter set.

CPU-Measurement Sampling Facility Authorization Controls
CPU-measurement sampling facility provides a means to take a snapshot of the CPU at a specified sampling interval. Select this option only when you want to collect measurement data for performance statistics.

Access basic sampling
Select this option to authorize the use of the basic sampling function. Samples are taken and stored at the end of each sampling interval. If you select this option, the Controls display changes to enable you to select an additional option: **Access diagnostic sampling**, which authorizes the use of the diagnostic sampling function.

Processors

Partitions on a DPM system can have only one defined processor type: either Central Processor (CP) or Integrated Facility for Linux (IFL), depending on the processor types that are installed on the system. Use the Processors section to view or modify the type, mode and number of virtual processors for the partition, and to view various charts that are based on your selections. The processor charts displayed are based on the processor mode that you select. The virtual processors are allocated from physical processors of the selected type.

The following list provides a description of each element in the Processors section. On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Processor type
If this field is displayed in the Processors section, the value indicates the currently selected processor type, which is either the **Central Processor (CP)** or **Integrated Facility for Linux (IFL)** processor type. If only one type of processor is installed on the system, this field is not displayed. If the partition is currently active, you cannot modify the selected type. Note that simultaneous multithreading is supported only for the IFL processor type.

Processor mode
Indicates the currently selected processor mode. If the partition is currently active, you cannot modify the selected mode.

Shared
Select this option when you want the new partition to share processor resources from the pool of physical processors that are not dedicated to other partitions.

Dedicated
Select this option when you want the new partition to have exclusive use of a specific number of physical processors installed on the system..

Processors
Indicates the currently defined number of shared or dedicated processors for the partition. You can use one of the following controls to modify the value.

Slider

The minimum value is 1 and the maximum value is the number of entitled processors on the system. The slider not only shows the total range of values that you can select, but also uses color to indicate the current state of processor resources on the system. The slider ranges and colors vary, depending on whether the partition is currently stopped or active.

When the partition is stopped

The slider displays two ranges: one range on the left, highlighted in green, and the other range on the right, highlighted in yellow or red.

- Green indicates the range of available processor resources. If you select a value in this range, you can successfully start the partition.
- Yellow or red indicate the range of processor values that prevent the new partition from starting, or prevent the partition from receiving its required amount of processor resources. This range has a different significance, depending on the selected processor mode and whether you have selected the **Reserve resources** check box in the General section.

  For shared processor mode

  When the processor mode is shared, this range is the number of dedicated processors that are assigned to active and reserved partitions. If you select a number in this range, you receive an inline warning or error message indicating that the processor value you selected is greater than the number of shared physical processors.

  – If you have not selected **Reserve resources**, this range is highlighted in yellow and you receive an inline warning message about your selection. In this case, the partition cannot be started unless the number of shared physical processors on the system is increased.

  – If you have selected **Reserve resources**, this range is highlighted in red and you receive an inline error message about your selection. In this case, the partition might successfully start, but its processor resources cannot be reserved unless the number of shared physical processors on the system is increased.

  For dedicated processor mode

  When the processor mode is dedicated, this range is the sum of the number of dedicated processors assigned to active and reserved partitions, plus the minimum number of shared physical processors required (that is, the largest number of shared processors that is assigned to a single active or reserved partition). If you select a number in this range, the inline warning or error message indicates that the processor value you selected is greater than the number of available physical processors.

  – If you have not selected **Reserve resources**, this range is highlighted in yellow and you receive an inline warning message about your selection. In this case, the partition cannot be started unless the number of dedicated physical processors on the system is increased.

  – If you have selected **Reserve resources**, this range is highlighted in red and you receive an inline error message about your selection. In this case, the partition might successfully start, but its processor resources cannot be reserved unless the number of dedicated physical processors on the system is increased.

When the partition is active

The slider displays three ranges: one range starting on the left, highlighted in red; another range in the middle, highlighted in green; and the final range on the right, highlighted in red.

- Green indicates the range of available processor resources that you can successfully select.
- Red indicates processor resources that are not available for use. If you try to select a number in one of the ranges highlighted in red, an error message is displayed.

  – The first range, on the left, indicates the number of processors that have been varied on by the hypervisor or operating system running on the partition. You cannot select fewer processors than the number that this partition is already using.

- The other range, on the right, indicates the number of shared or dedicated processors that are assigned to active and reserved partitions. These processors are not available for use.

Text entry box and number spinner
Using the text box, enter a valid integer within the limits of the slider range. When you enter a value, the slider changes to reflect the value entered in the text box. Alternatively, use the number spinner to increment or decrement the value in the text entry box and slider. Each click increments or decrements the value by one, within the limits of the slider range.

Threads
Indicates the number of threads that are available for use when simultaneous multithreading (SMT) is enabled, and when the processor type for the partition is **Integrated Facility for Linux (IFL)**. DPM displays thread information only under the following circumstances:

- When an administrator has explicitly enabled SMT, or when SMT is enabled by default, for the operating system or hypervisor that runs on the partition.
- When DPM can retrieve SMT information from the operating system or hypervisor that runs on the partition. If the partition is stopped, for example, DPM cannot display thread information.

Processors bar chart
Indicates the number of shared and dedicated physical processors on the system. The bar chart scale ranges from 0 to the system design limit. To show the actual number of processors that each bar segment represents, hover your cursor over the colored segment. A dotted line indicates the total number of entitled processors on the system. Entitled processors are processors that are licensed for use on the system; the number of entitled processors might be less than the total number of physical processors that are installed on the system.

To the right of the bar chart, a color legend identifies each segment of the bar chart:

- The number of shared or dedicated processors that you have currently specified for the new partition. This value varies when you change the Processors setting through the slider, text box, or number spinner.
- The number of shared processors, if any, that are available for use by partitions on the system.
- The number of dedicated physical processors that are assigned to active partitions and reserved partitions, if any exist. This number does not reflect any dedicated processors that are assigned to stopped or unreserved partitions.
- The total number of entitled processors on the system. If you have specified a number in the second range (yellow) for the new partition, the total number of processors for all partitions might exceed the number of entitled processors.

Shared Processors pie chart
Indicates the relative distribution of virtual processors for this new partition and all active partitions on the system that are using shared physical processors. This pie chart is displayed only when you have selected Shared as the processor mode.

To the right of the pie chart, a color legend identifies each of the partitions by name. To view details for a specific partition in the pie chart, hover your cursor over the pie wedge with the same color as shown in the legend, next to the partition name. The pie wedge is slightly enlarged and a tooltip displays details for the partition. The tooltip displays the partition name, the number of processors for that partition, and its relative percentage of the total shared partitions, rounded to two decimal places.

At most, the pie chart consists of 12 wedges, one of which is reserved for this new partition. If the system has more than 11 active partitions, the pie chart is divided as follows:

- One wedge for the new partition that you are defining. The wedge size and number of processors vary when you change the Processors setting through the slider, text box, or number spinner.
- One wedge for each of the 10 active partitions with the highest number of processors.
- One wedge that represents all remaining active partitions on the system and the total number of processors shared by this group. In the legend, this group wedge is labeled Others, with the total number of partitions in parentheses.

Processing weight
Select the relative amount of processor time that a specific active partition receives when it is in contention with other active partitions that share the same pool of processor resources. Processing weight options, and a link that opens the **Manage Processor Sharing** task, are displayed only when you have selected Shared as the processor mode.

The processing weight scale ranges from 1 to 999, with specific values labeled as Very Low (100), Low (300), Medium (500), High (700), and Very High (900). These labels are hyperlinks that you can select. Use either the vertical slider on the scale, the hyperlink labels, the text box, or the number spinner to select a value. If you use the number spinner, each click increments or decrements the value by one. The suggested practice is to specify a processing weight that satisfies the peak workload requirements of the partition.

Enforce weight capping
Select this option to enforce weight capping for the partition. When weight capping is enforced, the partition cannot use more processor time than its weight, relative to other partitions that share the same pool of processor resources, even when additional processor resources are available.

Enforce absolute processor capping
Select this option to enforce absolute processor capping for the partition. When absolute capping is enforced, this partition cannot use any more than a specific number of physical processors when it is active. When you select this option, you can enter the absolute capping value, which is the maximum number of physical processors that this partition can use. The absolute capping value ranges from 0.01 - 255.0, in increments of 0.01.

Active Processing Weights pie chart
Indicates the relative distribution of processor weights for this partition and all active partitions on the system. This pie chart is displayed only when you have selected Shared as the processor mode.

To the right of the pie chart, a color legend identifies each of the partitions by name. To view details for a specific partition in the pie chart, hover your cursor over the pie wedge with the same color as shown in the legend, next to the partition name. The pie wedge is slightly enlarged and a tooltip displays details for the partition. The tooltip displays the partition name, its weight value, and its relative percentage of the total processing weight, rounded to two decimal places.

Manage Processor Sharing
Launches the **Manage Processor Sharing** task, which provides the controls through which you can set weights, weight capping, and absolute capping for partitions with shared processors.

Memory

Each partition on a DPM-enabled system has exclusive use of a user-defined portion of the total amount of entitled memory that is installed on the system. Use the Memory page to view or modify the initial and maximum amounts of memory that are assigned to a specific partition.

When you define the amount of memory to be assigned, or allocated, to a specific partition, you specify an initial amount of memory, and a maximum amount that must be equal to or greater than the initial amount. The partition receives its initial amount when it is started. If the maximum amount of memory is greater than the initial amount, you can add memory up to this maximum to the active partition, without stopping and restarting it.

The following list provides a description of each element in the Memory section. On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional. You can set the memory amounts in different units: megabytes (MB), gigabytes (GB), or terabytes (TB). The default unit is GB. To change the unit, hover your cursor over the unit in a field label, and select another unit from the popup display. When you change the unit for one field, the same unit change is replicated to the other display elements on the page.

Memory
Specifies the amount of memory that is currently assigned to the partition. This value represents the initial amount of memory that the partition receives when it is started. If you set this initial amount to a value greater than the value currently displayed for the Maximum Memory field, the maximum memory is automatically set to the same value. When the partition is not active, you can use one

of the following controls to modify the value. If you are modifying the value for a Secure Service Container partition, you must specify an initial amount of at least 4096 MB (4 GB).

Slider

The minimum value that is displayed depends on the unit that you have selected (MB, GB, or TB); for example, the minimum value for the default unit (GB) is 0.5. The maximum value is the amount of entitled memory on the system; this maximum varies by system. The slider not only shows the total range of values that you can select, but also uses color to indicate the current state of memory resources on the system. The slider ranges and colors vary, depending on whether the partition is currently stopped or active.

When the partition is stopped

The slider displays two ranges: one range on the left, highlighted in green, and the other range on the right, highlighted in yellow or red.

- Green indicates the range of available memory values that you can select and successfully assign to the partition.
- Yellow or red indicate the range of memory values that might prevent the partition from starting, or prevent the partition from receiving its required amount of memory resources. This range is the amount of memory that is assigned to active and reserved partitions; it has a different significance, depending on whether you have selected the **Reserve resources** check box in the General section.
  - If you have not selected **Reserve resources**, this range is highlighted in yellow and you receive an inline warning message about your selection. In this case, the partition might fail to start until the amount of available memory on the system is increased.
  - If you have selected **Reserve resources**, this range is highlighted in red and you receive an inline error message about your selection. In this case, the partition might successfully start, but its memory resources cannot be reserved unless the amount of available memory on the system is increased.

When the partition is active

The slider displays three ranges: one range starting on the left, highlighted in red; another range in the middle, highlighted in green; and the final range on the right, highlighted in red.

- Green indicates the range of available memory that you can successfully select.
- Red indicates memory resources that are not available for use. If you try to select a number in one of the ranges highlighted in red, an error message is displayed.
  - The first range, on the left, indicates the amount of memory that is allocated by the hypervisor or operating system running on the partition. You cannot select less memory than the amount that this partition is already using.
  - The other range, on the right, indicates the amount of memory that is assigned to active and reserved partitions.

Text entry box and number spinner

Using the text box, enter a valid integer within the limits of the slider range. When you enter a value, the slider changes to reflect the value entered in the text box. Alternatively, use the number spinner to increment or decrement the value in the text entry box and slider. Each click increments or decrements the value by 0.5, within the limits of the slider range.

Maximum Memory

Specifies the amount of maximum memory assigned to the partition. When the partition is not active, you can change the current value; the new value that you specify must be equal to or greater than the value specified in the Memory field.

The controls (slider, text box and number spinner) are the same as those for the Memory field; however, these controls are disabled when the partition is active. The slider ranges and colors also have the same significance as those for the Memory field.

Installed Memory bar chart
Indicates the distribution and amounts of system memory, including the memory assigned to this partition. The bar chart scale ranges from 0 to the total amount of memory that is installed on the system. To show the actual amount of memory that each bar segment represents, hover your cursor over the colored segment.

To the right of the bar chart, a color legend identifies each segment of the bar chart:

- The amount of memory that you have currently specified for this partition. This value varies when you change the Memory setting through the slider, text box, or number spinner.
- The maximum amount of memory that you have currently specified for this partition. This value is represented as a dotted line in the bar chart, and its position moves when you change the Maximum Memory setting through the slider, text box, or number spinner.
- The total amount of allocated memory, which is the total memory assigned to all active and reserved partitions on this system.
- The amount of entitled memory for this system. Entitled memory is the amount of memory that is licensed for use, which might be less than the total amount of memory that is installed on the system. This value is represented as a dotted line in the bar chart.

Network

Network interface cards (NICs) provide a partition with access to internal or external networks that are part of or connected to a system. Each NIC represents a unique connection between the partition and a specific network adapter that is defined or installed on the system.

Use the Network section to view, to modify, or to create NICs that enable the partition to access the networks connected to the DPM-enabled system. When you create a NIC, you can select the adapter that you want to use from a list of all of the network adapters that are currently configured on the system.

- For availability, select at least two network adapters of the same type, and create a NIC for each one.
- For a Secure Service Container partition, you must specify at least one NIC for communication with the Secure Service Container web interface.

The following topics describe the NICs table actions and elements, and the elements in the "Secure Service Container Web Interface Communication" section, which is displayed only for Secure Service Container partitions.

- “The NICs table toolbar” on page 705
- “Columns in the NICs table” on page 706
- “Standard table functions” on page 707
- “Secure Service Container Web Interface Communication” on page 708

The NICs table toolbar

The NICs table contains an entry for each network interface card, if any, that has been defined for this new partition.

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both.

New
Opens the **New Network Interface Card** window, through which you can create a new network interface card. For more information, see “New Network Interface Card” on page 708.

Details
Opens the **NIC Details** window. This action is enabled when only one NIC is selected in the table. The **NIC Details** window fields and controls are the same as those for the **New Network Interface Card** window, with the following exceptions:

- The name, description (if any), device number, and adapter port or switch selection are displayed for the selected NIC.
- The Device number field is marked as a required field.
- If the NIC is the only NIC that provides access to the Secure Service Container web interface, the "Use to access the web interface" switch is set on and cannot be set off.
- The Adapter Ports and Switches table contains entries for only those configured ports and switches that have the same card type as the selected NIC, because you cannot change the type of network interface card.

If you plan to change either the VLAN ID or the MAC address of this NIC, note the following:

- If you change either the VLAN ID value or the MAC address after the partition is created and started, the NIC is deactivated and reactivated, which is disruptive to any network activity taking place over this device in the operating system or hypervisor.
- If you change VLAN ID value, make sure that you also use the new VLAN ID value in the network configuration files for the operating system or hypervisor.

Delete
Opens the **Delete NIC** confirmation window through which you can delete one or more NICs. This action is enabled when one or more NICs are selected in the table.

Note that, for a Secure Service Container partition, DPM does not process the delete operation if the end result is that all defined NICs are removed. For this type of partition, at least one NIC is required to access the Secure Service Container web interface.

In the confirmation window, click one of the following buttons:

- Click **Delete** to confirm that you want to delete the selected NICs. The confirmation window closes, and the resulting NICs table display does not contain any entries for the deleted NICs. The NICs are not actually deleted until you click **OK** or **Apply** on the main window of the **Partition Details** task.
- Click **Cancel** to close the confirmation window and return to the Network section, without deleting any NICs.

Adapter Details
Opens the **Adapter Details** task in a separate window. This action is enabled when one or more NICs are selected in the table.

Columns in the NICs table

The NICs table contains the following columns in the default display. You can modify the columns in the default table display by using the **Configure Options** icon or action.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of a virtual network interface card (NIC). The name is a hyperlink through which you can open the **NIC Details** window. To edit the name, double-click in the table cell and type the new name.

If this NIC represents an adapter that might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

IP Address
Displays one of the following values:

- For a NIC that provides access to the Secure Service Container web interface, the value is either a specific IPv4 or IPv6 address or, for IP address types of DHCP and Link Local, the word Automatic.
- For all other NICs, the value displayed is a dash (-).

Device Number
Displays the user-supplied or system-generated hexadecimal device number for the NIC. The operating system to be installed on the partition will use this device number to access the NIC. When creating a new NIC for an OSA card or HiperSockets switch, DPM generates three consecutive device numbers for the operating system to use for unit addresses, and displays only the first number in this field.

Change the device number if your company uses a specific numbering convention for its networks. To edit the device number, double-click in the table cell and type a new hexadecimal value. When you edit the device number for an OSA card or HiperSockets switch, DPM uses this new value as the first device number, and generates two consecutive device numbers based on the new value.

Notes:

- You cannot use a device number of 0000 for a PCI adapter, such as a RoCE adapter.
- The z/VM hypervisor does not support a device number of 0000 for an OSA card or HiperSockets switch.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Adapter Port
Displays the adapter port value in decimal.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include HiperSockets, or specific OSA Express or RoCE Express adapter names.

VLAN ID & Type
Displays the identifier of the virtual local area network (VLAN) through which the network adapter sends and receives network traffic. This field also displays the type of VLAN configuration, such as VLAN Enforcement.

MAC Address
Displays the user-provided or system-generated unique media access control (MAC) address for this NIC.

Description
Displays the user-provided description, if any, of the network interface card. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

Standard table functions

In addition to the customized action icons and the Actions list, the table toolbar includes the following standard table functions.

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Advanced Filter
Provides advanced filter options through which you can reduce the total number of table entries. To access filter options, click the Filter icon ().

Secure Service Container Web Interface Communication

The "Secure Service Container Web Interface Communication" section displays network settings for a Secure Service Container partition. Some of the displayed values depend on the IP address type of the NIC that provides access to the web interface. An asterisk (*) preceding the label indicates that a value is required. These fields are read-only until you click **RESET NETWORK**.

Host Name
Specifies the Linux host name of the appliance to run in the Secure Service Container partition. To access the Secure Service Container web interface, users need to specify a URL that contains either a host name or an IP address for the Secure Service Container partition. A host name can be 1 - 32 characters long. It cannot contain blanks. Valid characters are numbers 0 - 9, letters A - Z (any case), and the following special characters: period (.), colon (:), and hyphen (-).

Default IPv4 Gateway
Specifies an IPv4 address for the default gateway. A default IPv4 gateway is required if you specified a Static IPv4 IP address type for the NIC.

Default IPv6 Gateway
Specifies an IPv6 address for the default gateway. A default IPv6 gateway is required if you specified a Static IPv6 IP address type for the NIC.

DNS Server 1
Specifies an IPv4 or IPv6 address for the primary domain name system (DNS) server. A DNS server definition is required if you specified a Dynamic Host Configuration Protocol (DHCP) IP address for the NIC.

DNS Server 2
Specifies an IPv4 or IPv6 address for a secondary DNS server.

RESET NETWORK
Click **RESET NETWORK** to remove any previously supplied values for fields in the "Secure Service Container Web Interface Communication" section, so you can supply new values. To save the new values and associate them with the NIC that provides access to the web interface, click **Apply**; otherwise, click **Cancel** to cancel the reset operation.

New Network Interface Card

Use the **New Network Interface Card** window to create a network interface card (NIC). On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Name
Initially displays a system-generated name for the new NIC, which you can edit by double-clicking in the name field and typing a new name. The NIC name must be different from the name of any other NIC that you define for this new partition.

Description
Optionally, provide a description for this new NIC. The description can be up to 1024 characters in length.

Device Number
Optionally, provide a 4-digit hexadecimal device number in the range 0000 - ffff. If you do not provide a value, the system automatically generates a unique device number. When creating a new NIC for an OSA card or HiperSockets switch, DPM generates three consecutive device numbers for the operating system to use for unit addresses; if you supply a value, the system uses this value as the first device number.

For a NIC that is backed by a PCI-based adapter, DPM generates a unique identifier (UID) that is used as the PCI device number. The value is used only if the operating system supports PCI device numbers.

VLAN ID
For partitions with a type of **Linux** or **z/VM** only, optionally specify the identifier of the virtual local area network (VLAN) through which the network adapter is to send and receive network traffic for this partition and the operating system or hypervisor that it hosts.

- The valid range of VLAN IDs is 1 - 4094.
- You can specify a VLAN ID for this NIC only when you select an OSA-Express or HiperSockets adapter.

  This field is not displayed for partitions with a type of **Secure Service Container**, but you can specify a VLAN ID for that partition type by setting the **Use to access the web interface** switch to **YES**, and entering a value in the **VLAN ID** field displayed in the section under that switch.

VLAN Type
If you provide a VLAN ID, this field, which specifies the type of VLAN configuration, is displayed. The default value is VLAN Enforcement. To complete the setup for VLAN enforcement, you must specify the same VLAN ID in the network configuration files for the operating system or hypervisor.

MAC Address
Optionally, specify a unique media access control (MAC) address that is both locally administered and unicast. A MAC address consists of six groups of two lower-case hexadecimal digits, separated by colons; for example: `12:34:56:78:9a:bc`

You can specify a MAC address for any type of partition, but only when you select an OSA-Express or HiperSockets adapter for the NIC. DPM checks the validity and uniqueness of the value that you supply, and issues a message if it finds an error. If you do not specify a value, DPM automatically generates a unique MAC address for the NIC.

Use to access the web interface
Only when the partition type of this partition is **Secure Service Container**, the display includes a switch to indicate whether you can configure this NIC to access the Secure Service Container web interface. If this NIC is the only NIC defined for this Secure Service Container partition, you cannot set this switch to **NO**. When the switch is set to **YES**, the display includes the following configuration settings, which Secure Service Container partitions require for access to the web interface. For a Secure Service Container partition, you can select only an OSA or HiperSockets adapter.

VLAN ID
Specify the virtual local area network (VLAN) if the link you are using is defined in TRUNK mode. The valid range of VLAN IDs is 1 - 4094. Note that DPM does not provide VLAN enforcement for Secure Service Container partitions.

IP Address Type
Select one of the following types:

- **DHCP** (Dynamic Host Configuration Protocol)
- **Link Local**
- **Static IPv4 Address**
- **Static IPv6 Address**

The selected type determines which of the remaining fields require values. An asterisk (*) preceding the label indicates that a value is required.

IP Address
Enter the IP address of the network adapter. This field is required only for IP addresses of type **Static IPv4 Address** and **Static IPv6 Address**.

Mask/Prefix
For an IPv4 address type, enter the mask/prefix in either bit notation (for example, /24) or mask notation (for example, 255.255.255.0). For an IPv6 address type, enter the mask/prefix in bit notation only.

Adapter Ports and Switches table
Lists all of the configured ports or switches for all of the configured network adapters on this system. To successfully define a new NIC, you must select only one table entry.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. Select only one adapter port or switch for the new NIC.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Adapter Port
Displays the adapter port value in decimal.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include HiperSockets, or specific OSA Express or RoCE Express adapter names.

Uplink Utilization
Indicates the average uplink utilization for the port or switch over the last five minutes. If the percentage is high (for example, 90%), consider selecting a different port or switch on the same network. The utilization is shown in both a graphic progress bar and in numeric percentage. For OSA and RoCE adapters, the physical port utilization is displayed; for HiperSockets, the switch utilization is displayed.

Adapter NIC Allocation
Indicates the percentage of NICs that are currently allocated to the adapter for this port or switch. If the percentage is high (for example, 90%), consider selecting a different port or switch on the same network. The percentage is shown in both a graphic progress bar and in numeric format. The displayed percentage includes NICs only for started and reserved partitions. To display this numeric percentage along with the numeric percentage for all partitions, hover your cursor over the column cell. The percentage for all partitions can exceed 100%.

Each network adapter port or switch has enough allocation space to support a maximum number of NICs; the maximum number varies depending on the adapter type. If you select a port or switch on an adapter that does not have sufficient allocation space for this new NIC, a message is displayed above the table:

- If the partition is active or if you have selected the **Reserve resources** check box in the General section, the message reports an error. In this case, you must select a port or switch on a different adapter.
- If the partition is stopped and you have not selected the **Reserve resources** check box, the message is only a warning that your new partition might not be successfully started because the adapter does not have sufficient allocation space.

Location
Provides the location of the adapter in the I/O cage of the system.

Description
Displays the user-provided description, if any, of the port or adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

OK
After you have supplied all of the required values for the new NIC, click **OK** to create the NIC definition and close the **New Network Interface Card** window.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Storage

Use the Storage section to view, to modify, or to attach storage groups and tape links, or to create host bus adapters (HBAs), that enable the partition to access storage networks and hardware that is connected to the DPM-enabled system.

Depending on the version of DPM that is applied on the system, the Storage section contains a Storage Groups table, a Tape Links table, or an HBAs table with controls that you can use to attach storage groups and tape links, or to create HBAs. Follow the instructions that correspond to the type of table displayed on the page.

- "Viewing or modifying attached storage groups or tape links (DPM R3.1 or later)" on page 711
- "Viewing or modifying HBAs for FCP storage access (DPM R3.0 or earlier)" on page 714

Viewing or modifying attached storage groups or tape links (DPM R3.1 or later)

System administrators create storage groups and tape links to enable partitions (and the operating systems and applications that they host) to use physical storage hardware that is connected to the system. A *storage group* is a logical group of storage volumes that share certain attributes. A *tape link* defines the attributes of a connection that one or more partitions can use to access one FCP tape library in the SAN.

DPM supports the following types of storage groups and tape links.

- FICON storage groups, which consist of volumes that reside on external Fibre Connection (FICON) extended count key data (ECKD) direct-access storage devices (DASD). This type of storage group is available starting with DPM R3.1.
- FCP storage groups, which consist of volumes that reside on external Fibre Channel Protocol (FCP) Small Computer System Interface (SCSI) disk storage devices. This type of storage group is available starting with DPM R3.1.
- Non-Volatile Memory Express (NVMe) storage groups, which consist of solid state drives (SSDs) that are installed in carrier cards in the system I/O drawers. NVMe storage is available only when the system has one or more IBM Adapter for NVMe1.1 feature. This type of storage group is available starting with DPM R4.2.
- FCP tape links, each of which defines the attributes of a connection that one or more partitions can use to access one FCP tape library in the SAN. These connection attributes include storage resources such as system adapters, world wide port names (WWPNs), and the number of partitions that can share the connection. Support for FCP tape links is available starting with DPM R4.3.

FCP storage groups can be shared by multiple partitions, and multiple storage groups can be attached to one partition. FCP tape links also can be shared by multiple partitions, and multiple tape links can be attached to one partition. In contrast, only one partition can use an NVMe storage group at any given time; an NVMe storage group cannot be shared. However, a partition that has attached NVMe storage groups can also have attached FICON and FCP storage groups, and FCP tape links.

To attach new storage groups or tape links to the partition, complete the following steps.

1. Select the plus icon in the table toolbar to open the **Attach Storage Groups** or **Attach Tape Links** window. (Note that you can use the minus icon in the table toolbar to detach a storage group or tape link from the partition.)
   - On the **Attach Storage Groups** window, select one or more storage groups listed in the Storage Groups table to attach to this partition.

  - The suggested practice is to select storage groups that are in the Complete fulfillment state, but you can select any storage group except for those with a fulfillment state of Incomplete, or those that are already attached to the maximum number of partitions. If you do select groups in states other than Complete, some storage might not be available for use when you start the partition.
  - Use the additional information in the Storage Groups table, as necessary, to decide which storage groups to attach. For descriptions of the columns in the Storage Groups table, see "Attach Storage Groups" on page 716.

  When you have finished selecting storage groups to attach, select **OK** to close the **Attach Storage Groups** window.

- On the **Attach Tape Links** window, select one or more tape links listed in the table to attach to this partition.
  - The suggested practice is to select tape links that are in the Complete fulfillment state, but you can select any tape link except for those with a fulfillment state of Incomplete, or those that are already attached to the maximum number of partitions. If you do select links in states other than Complete, some storage might not be available for use when you start the partition.
  - Use the additional information in the table, as necessary, to decide which tape links to attach. For descriptions of the columns in the table, see "Attach Tape Links" on page 717.

  When you have finished selecting tape links to attach, select **OK** to close the **Attach Tape Links** window.

2. Check the entries for the storage groups or tape links that you selected, which are now displayed in the Storage Groups table or Tape Links table in the Storage section. If necessary, you can use the minus icon in the table toolbar to remove a storage group or tape link from the table.
   - For FICON storage groups only, you can change the volume device numbers only when the device number input field is active. The factors that determine whether you can change the device number include not only the current state of the partition, but also whether the storage group is shared or dedicated, and whether it is already attached to other partitions.
   - For FCP storage groups and FCP tape links only, you can expand the table entry to show the system-generated host bus adapters (HBAs) and their assigned adapters. You can change the device numbers that DPM automatically assigned to the HBAs when you selected the FCP storage group or FCP tape link. An error icon is displayed if you try to specify a device number that is already in use.
   - For FCP storage groups only, the expanded display also includes a link through which you can open the FCP adapter assignment window, and remove or replace the adapters that DPM automatically assigned to the HBAs.

   For more details, see the following topics.

   - "Host Bus Adapters (HBA) table for an FCP storage group or tape link" on page 713
   - "FCP adapter assignment" on page 718
3. When you have finished, review another section or click **OK** to save the partition definition.

   If the partition is running, or when you restart a stopped partition, you might need to enter Linux commands to make any newly attached storage groups available to the operating system that the partition hosts. NVMe storage groups are automatically detected by the operating system, so you do not need to enter Linux commands to make that type of storage group available to the operating system. Similarly, the tape devices that are available through attached tape links are automatically detected by the operating system, so you do not need to enter Linux commands for tape devices either. The actions required for FCP or FICON storage groups depend on the type and fulfillment state, and whether the storage group contained the boot volume for the operating system.

   When attaching a storage group in Complete state when the partition is stopped

   - For an FCP storage group:
     - If the storage group contained the boot volume, the operating system brings online all of the HBAs for this storage group, and all volumes in the storage group are available. No action is required unless you have attached other storage groups.

  - If the storage group does not contain the boot volume, and the operating system is not configured to bring HBAs online automatically, you need to issue the **chccwdev** command to bring online all of the HBAs.
- For a FICON storage group, the operating system brings online only the boot volume. You need to issue the **chccwdev** command to bring online all of the remaining volumes in the storage group that contains the boot volume, as well as the volumes in any other storage groups that you attached.

When attaching a Complete storage group to a running partition, or attaching an unfulfilled storage group that becomes Complete as the partition is running

- For an FCP storage group:
  - If adapters were assigned to HBAs while the partition is running, you need to use the **chchp** command to activate the channel paths for those new adapters.
  - To access the volumes in the storage group, you need to issue the **chccwdev** command to bring online all of the HBAs.
- For a FICON storage group:
  - If the adapters connecting the storage group to the storage subsystem were assigned while the partition is running, use the **chchp** command to activate the channel paths for those new adapters.
  - All volumes are offline. You need to issue the **chccwdev** command to bring online all of the volumes in the storage group.

To find the IDs that you need to use for the Linux commands, use the following tasks.

- HBA device numbers are available in the Host Bus Adapters (HBA) table when you expand the storage group table entry in the Storage section of the **Partition Details** task.
- Channel path IDs for FCP adapters are shown in the Host Bus Adapters (HBA) table when you expand the storage group table entry in the Storage section of the **Partition Details** task.
- Channel path IDs for FICON adapters are shown on the **ADAPTERS** tab of the Storage Group details; open the **Configure Storage** task and select the storage group in the **Storage Overview** to open the Storage Group details page.
- FICON volume device numbers are shown on the **VOLUMES** tab of the Storage Group details page; open the **Configure Storage** task and select the storage group in the **Storage Overview** to open the Storage Group details page.

Host Bus Adapters (HBA) table for an FCP storage group or tape link

For FCP storage groups or tape links only, you can expand the Storage Groups or Tape Links table entry to show the Host Bus Adapters (HBA) table. The following list describes the columns in the table; depending on the fulfillment state of the storage group or tape link, some information might not be available.

Name
Displays the system-generated name of the HBA.

Device Number
Displays the system-generated hexadecimal device number for the HBA. If your company uses a specific numbering convention for its storage networks, you can change a system-generated device number by typing a new value in the column field.

WWPN
Specifies the 16-character hexadecimal string (64-bit binary number) that uniquely identifies a port in a disk storage subsystem or tape library that is connected to the system.

Fabric ID
Displays the worldwide name (WWN) of the uplink Fibre Channel switch.

Adapter ID
Specifies the physical channel ID of the adapter; this ID is a four-character hexadecimal number.

Assigned Adapter
Specifies the name of the adapter. The name is a hyperlink through which you can open **Adapter Details** in the **Manage Adapters** task.

Viewing or modifying HBAs for FCP storage access (DPM R3.0 or earlier)

Host bus adapters (HBAs) provide a partition with access to external storage area networks (SANs) and devices that are connected to a system. Each HBA represents a unique connection between the partition and a physical FICON channel that is configured on the system. When you modify or create an HBA, you can select the adapter that you want to use from a list of all of the storage adapters that are currently configured on the system.

- For availability, select at least two storage adapters of the same type, and create an HBA for each one.
- If you are creating a Secure Service Container partition to install a software appliance, define at least one HBA to access the storage device on which the appliance installation image resides.

The following topics describe the HBAs table actions and elements.

- "The HBAs table toolbar" on page 714
- "Columns in the HBAs table" on page 715
- "Standard table functions" on page 715

The HBAs table toolbar

The HBAs table contains an entry for each host bus adapter, if any, that has been defined for this new partition.

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both.

New
Opens the **New Host Bus Adapter** window, through which you can create a new host bus adapter (HBA). For more information, see "New Host Bus Adapter" on page 719.

Details
Opens the **HBA Details** window. This action is enabled when only one HBA is selected in the table. The **HBA Details** window fields and controls are the same as those for the **New Host Bus Adapter** window, with the following exceptions:

- The name, description (if any), device number, and adapter port selection are displayed for the selected HBA.
- The read-only WWPN field displays the worldwide port name of the HBA. A WWPN is automatically assigned to an HBA when the HBA is created, and provides a unique identifier for it in the network.
- The Device number field is marked as a required field.

Delete
Opens the **Delete HBA** confirmation window through which you can delete one or more HBAs. This action is enabled when one or more HBAs are selected in the table.

In the confirmation window, click one of the following buttons:

- Click **Delete** to confirm that you want to delete the selected HBAs. The confirmation window closes, and the resulting HBAs table display does not contain any entries for the deleted HBAs. The HBAs are not actually deleted until you click **OK** or **Apply** on the main window of the **Partition Details** task.
- Click **Cancel** to close the confirmation window and return to the Storage section, without deleting any HBAs.

Adapter Details
Opens the **Adapter Details** task in a separate window. This action is enabled when one or more HBAs are selected in the table.

Columns in the HBAs table

The HBAs table contains the following columns in the default display. You can modify the columns in the default table display by using the **Configure Options** icon or action.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of a host bus adapter (HBA). The name is a hyperlink through which you can open the **HBA Details** window. To edit the name, double-click in the table cell and type the new name.

If this HBA represents an adapter that might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

WWPN
Displays the worldwide port name of the HBA. A WWPN is automatically assigned to an HBA when the HBA is created, and provides a unique identifier for it in the network.

Type
Indicates the HBA type, which matches the type of adapter port that is selected when the HBA is created. The valid value is FCP, which represents Fibre Channel Protocol mode.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Device Number
Displays the user-supplied or system-generated hexadecimal device number for the HBA. The operating system to be installed on the partition will use this device number to access the HBA.
If your company uses a specific numbering convention for its storage networks, you can change a system-generated device number by selecting the **Details** action and editing the HBA device number. To edit the device number, double-click in the table cell and type a new hexadecimal value.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific FICON Express adapter names.

Description
Displays the user-provided description, if any, of the host bus adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

Standard table functions

In addition to the customized action icons and the Actions list, the table toolbar includes the following standard table functions.

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Advanced Filter
Provides advanced filter options through which you can reduce the total number of table entries. To access filter options, click the Filter icon ().

Attach Storage Groups
Use the **Attach Storage Groups** window to select one or more storage groups to attach to the partition. This window contains the Storage Groups table, which lists all storage groups that system administrators have defined for use by partitions on a system on which the DPM R3.1 storage management feature or a later DPM version is applied.

The Storage Groups table contains the following information and controls.

Select
Use check boxes in the Select column to identify which storage groups you want to attach to the partition. If a check box is disabled, either the storage group is attached to the maximum number of partitions, or you do not have permission to access the storage group.

Name
Specifies the user-defined name of the storage group. The name is a link that opens to the Storage Group details page in the Configure Storage task.

Type
Specifies the type of storage group: FICON, FCP, or NVMe.

Partitions
Specifies the number of partitions to which the storage group is attached.

Shareable
Specifies whether the storage group can be shared among partitions, or whether it is dedicated to only one partition.

Total Capacity
Specifies the total amount of storage in gibibytes (GiBs) that is assigned to the storage group.

Description
Specifies the user-provided description, if any, of this storage group.

Fulfillment state
Identifies the current state of the storage group. DPM runs a background check of storage resources for FCP storage groups and, if necessary, changes the fulfillment state. These checks are more frequent (every 10 minutes) for fulfillment states other than Complete (every 24 hours)..

Checking migration
This fulfillment state indicates that DPM is checking the logical and physical elements that support a storage group it created during a system migration or firmware upgrade process.

Complete
The storage group is ready for use.

Incomplete
One or more volumes or adapters that are used for a storage group are marked as incomplete. DPM periodically checks the availability of storage volumes or adapters for storage groups, so resources that were functioning properly can become incomplete.

Pending
A system administrator has sent a request to create or modify a FICON or FCP storage group, but the storage administrator has not finished fulfilling that request through tools for managing storage subsystems.

Pending with mismatches
For an FCP storage group, a system administrator sent a request to create or modify that storage group, and the storage administrator fulfilled that request, but with an amount of storage that does not exactly match the original request. For an NVMe storage group, as part of a repair, one or more NVMe SSDs were replaced with SSDs of a different size.

Conflicts
Specifies whether any device numbers will be duplicated in the configuration if you attach a FICON storage group. This column contains a warning icon and message when one or more of the following conditions are true.

- One or more of the base or alias volume device numbers used in a FICON storage group are the same as a device number that is in use for this partition for a network connection through an OSA card or HiperSockets switch.
- One or more of the base or alias volume device numbers used in a FICON storage group are the same as a device number that is in use for one of the currently attached FICON or FCP storage groups.

To determine which device numbers conflict, select the chevron (⌄) to expand the table entry and display the Conflicting Device Numbers tables. One table identifies the device numbers for the storage group volumes, and another table lists the device numbers of configured partition resources that are in conflict. This second table lists the device number, device name, resource type, and a link to the task or page through which you can resolve the conflict.

To resolve conflicts, you can either change the conflicting device numbers, or remove the storage group. In some cases, you can edit the device numbers directly in the Conflicting Device Numbers tables. The Device Number column fields in both tables are editable depending on the shareability of the FICON storage group, whether the storage group is already attached to the partition, and the current state of the partition.

OK
After you have selected one or more storage groups, click **OK** to return to the Storage section of the **Partition Details** task.

CANCEL
To close the window without saving any selections, click **CANCEL**.

Attach Tape Links
Use the **Attach Tape Links** window to select one or more tape links to attach to the partition. This window contains the a table listing all tape links that system administrators have defined for use by partitions on a system on which the DPM R3.1 storage management feature or a later DPM version is applied.

The table contains the following information and controls.

❒
Use check boxes in each table row or in the table header to identify which tape links you want to attach to the partition. If a check box is disabled, either the storage group is attached to the maximum number of partitions, or you do not have permission to access the storage group.

Name
Specifies the user-defined name of the tape link. The name is a hyperlink that opens to the Tape Link details page in the **Configure Storage** task.

Type
Specifies the type of tape link: FCP.

Partitions
Specifies the number of partitions to which the tape link is attached.

Shareable
Specifies whether the tape link can be shared among partitions, or whether it is dedicated to only one partition.

Description
Specifies the user-provided description, if any, of this tape link. The description can be up to 200 characters in length.

Fulfillment state
Identifies the current state of the tape link. DPM runs a background check of storage resources for FCP tape links and, if necessary, changes the fulfillment state. These checks are more frequent (every 10 minutes) for fulfillment states other than Complete (every 24 hours).

Complete
All of the storage resources listed in a create or modify request are available, properly configured and zoned, and DPM detects only those resources.

Incomplete
One or more storage resources for the tape link are marked as incomplete because the resource is missing, or in an error or degraded condition. Because DPM periodically checks the availability of storage adapters, switches, and tape libraries that are in use for a tape link, resources that were functioning properly can become incomplete.

Pending
One or more requested storage resources are not yet available or zoned correctly, or the tape link is not yet attached to all partitions that were specified in the original create request or a modify request.

Pending with mismatches
DPM detects system adapters that do not match the original create request or a modify request. Either the number of system adapters does not match the number of connecting paths, or the detected adapters do not match specific adapters that were assigned to the tape link.

OK
After you have selected one or more tape links, click **OK** to return to the Storage section of the **New Partition** task.

CANCEL
To close the window without saving any selections, click **CANCEL**.

FCP adapter assignment
Use the **FCP adapter assignment** window to review the adapters assigned to a storage group and remove or replace them with other adapters that are available for use by a partition. This window is available only on a system on which the DPM R3.1 storage management feature or a later DPM version is applied.

The **FCP adapter assignment** window displays two tables: Assigned Adapters and Adapter Candidates. Each table contains the same columns and has a footer that indicates the total number of adapters in the table. You might need to scroll to see all table entries, or use the Search field to filter the table entries. The search string applies to both tables. Note that any incomplete adapters are indicated by an incomplete icon ( ).

If an FCP adapter is configured while the storage group is attached to an active partition, DPM cannot detect and list the new adapter as available for use by any partition. To make sure that you can choose from a complete list of available adapters, stop all active partitions to which the storage group is attached, and select the **Connection Report** icon to start a background check of the available connections for this storage group. To view all partitions that are using the storage group, go to **Configure Storage** > **Storage Overview**, open the Storage Details page for the storage group, and select the **PARTITIONS** tab.

If you need to assign new adapters, the Assigned Adapters table contains a placeholder row for each required adapter. To fill those placeholders, use one of the following methods.

- Use the **Automatically assign** icon ( ) to have DPM automatically select redundant adapters across all fabrics. DPM selects the adapters with the lowest allocation percentage and the fastest card type.

- Use the buttons in the Action table column to manually change adapter assignments, one adapter at a time. The suggested practice is to assign at least two adapters from each fabric for redundancy.
  1. In the Assigned Adapters table, select **UNASSIGN** to remove individual adapters.
  2. In the Adapter Candidates table, select **ASSIGN** to assign different adapters. Newly assigned adapters are indicated by a blue dot next to the table row in the Assigned Adapters table.

If you need to change all of the currently assigned adapters, use the **Unassign all** icon () to empty the Assigned Adapters table. Then use either the **Automatically assign** icon or the Action buttons to assign new adapters.

When you have finished, select **SAVE** to return to the Storage section of the **Partition Details** task.

The following list describes the columns that are displayed in both of the tables on the **FCP adapter assignment** window.

Adapter Name
Specifies the name of the adapter. The name is a hyperlink through which you can open **Adapter Details** in the **Manage Adapters** task.

Adapter ID
Specifies the physical channel ID of the adapter; this ID is a four-character hexadecimal number.

Location
Specifies the physical location of the adapter in the I/O drawer of the system.

Fabric ID
Displays the worldwide name (WWN) of the uplink Fibre Channel switch.

Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific FICON Express adapter names.

Allocation
Indicates the percentage of host bus adapters (HBAs) that are currently allocated to this adapter, shown in a bar graph and in numeric format. The displayed percentage includes HBAs only for started and reserved partitions. If the percentage is high (for example, 90%), consider assigning a different adapter.

Action
Contains one of the following buttons.

- In the Assigned Adapters table, **UNASSIGN** removes the adapter in the table row and moves the table row into the Adapter Candidates table.
- In the Adapter Candidates table, **ASSIGN** assigns the adapter in the table row and moves the table row into the Assigned Adapters table.

New Host Bus Adapter

Use the **New Host Bus Adapter** window to create a new host bus adapter (HBA). On the page, an asterisk (*) preceding the label indicates that a value is required; other values are optional.

Name
Initially displays a system-generated name for the new HBA, which you can edit by double-clicking in the name field and typing a new name. The HBA name must be different from the name of any other HBA that you define for this new partition.

Description
Optionally, provide a description for this new HBA. The description can be up to 1024 characters in length.

Device number
Optionally, provide a 4-digit hexadecimal device number in the range 0000 - ffff. If you do not provide a value, the system automatically generates a unique device number.

Adapter Ports table
Lists all of the configured ports for all of the configured storage adapters on this system. To successfully define a new HBA, you must select only one table entry.

Adapter Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific FICON Express adapter names.

Adapter HBA Allocation
Indicates the percentage of HBAs that are currently allocated to this adapter. If the percentage is high (for example, 90%), consider selecting a different adapter port. The percentage is shown in both a graphic progress bar and in numeric format. The displayed percentage includes HBAs only for started and reserved partitions. To display this numeric percentage along with the numeric percentage for all partitions, hover your cursor over the column cell. The percentage for all partitions can exceed 100%.

Each storage adapter port has enough allocation space to support a maximum of 254 HBAs, but your system planner can change that maximum to a lower value. If you select an adapter port that does not have sufficient allocation space for this new HBA, a message is displayed above the table:

- If the partition is active or if you have selected the **Reserve resources** check box in the General section, the message reports an error. In this case, you must select a different adapter.
- If the partition is stopped and you have not selected the **Reserve resources** check box, the message is only a warning that your new partition might not be successfully started because the adapter does not have sufficient allocation space.

Fabric ID
Displays the worldwide name (WWN) of the uplink Fibre Channel switch.

Location
Displays the location of the adapter in the I/O cage of the system.

Description
Displays the user-provided description, if any, of the port or adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

OK
After you have supplied all of the required values for the new HBA, click **OK** to create the HBA definition and close the **New Host Bus Adapter** window.

Cancel
To close the window without saving any changes, click **Cancel**. If you have made changes but did not save them, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Cryptos

The term *cryptos* is a commonly used abbreviation for adapters that provide cryptographic processing functions. Use the Cryptos section to view or modify the cryptographic adapters and domains that are assigned to the partition, or to enable the partition to use the cryptographic adapters that it requires, to assign a usage domain and, optionally, to assign control domains. Usage domains provide access to cryptographic functions, and provide the ability to manage domains and keys. Control domains provide only the ability to manage domains and keys.

Crypto features are optional and, therefore, might not be installed on the system. If none are installed, the Cryptos section is disabled.

When crypto adapters are installed on a system, they are configured in either coprocessor or accelerator mode, depending on the type of cryptographic processing that is required by the applications that run on the system. Each coprocessor or accelerator contains a specific number of usage domains, identified by an index number, which contain an isolated set of master keys. When you create a new partition, you select only one usage domain index to assign to your partition, and that index assignment applies for each cryptographic adapter that your partition can access.

Depending on the type of crypto adapter that you select, you might also need to define one or more control domains.

Additionally, you can enable or disable the key import functions that are available through the CP Assist for Cryptographic Functions (CPACF) feature. CPACF supports clear and protected key encryption based on the Advanced Encryption Standard (AES) algorithm, and the Secure Hash Algorithm (SHA) with the Data Encryption Standard (DES) algorithm, and the Elliptic Curve Cryptography (ECC) algorithm. For operating systems and applications to take advantage of key encryption support, the partition in which they run must be configured to permit AES, or DES, or ECC protected key import functions.

The following topics describe the table actions and elements in the Cryptos section.

- "Fields for CPACF Key Management Operations" on page 721
- "The Adapters table toolbar" on page 721
- "Columns in the Adapters table" on page 722
- "The Adapter Domains table toolbar" on page 723
- "Columns in the Adapter Domains table" on page 723
- "Standard table functions" on page 724

Fields for CPACF Key Management Operations

Review the options for the CPACF Key Management Operations that are, by default, selected for this partition. If necessary, click the check box to deselect one or all options. Note that you cannot deselect a key import permission while the partition is active.

Permit AES key import functions
When selected, this option enables applications that run in this partition to generate and manage AES protected keys through the CPACF feature.

Permit DES key import functions
When selected, this option enables applications that run in this partition to generate and manage DES protected keys through the CPACF feature.

Permit ECC key import functions
When selected, this option enables applications that run in this partition to generate and manage ECC protected keys through the CPACF feature. Note that only specific systems support the ECC algorithm; if this system does not support ECC, this key import selection is disabled.

The Adapters table toolbar

The Adapters table contains an entry for each cryptographic coprocessor or accelerator, if any, that has been defined for this new partition.

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both.

Add
Opens the **Add Adapters** window through which you can add one or more crypto adapters to be used by the partition. For more information, see "Adding cryptographic adapters and domains" on page 724.

Remove
Opens the **Remove Adapters** confirmation window through which you can remove one or more adapters from the partition definition. This action is enabled when one or more adapters are selected in the table.

In the confirmation window, click one of the following buttons:

- Click **Remove** to confirm that you want to remove the selected adapters. The confirmation window closes, and the resulting Adapters table display does not contain any entries for the deleted adapters.
- Click **Cancel** to close the confirmation window and return to the Cryptos section, without removing any adapters.

Adapter Details
Opens the **Adapter Details** task. This action is enabled when one or more adapters are selected in the table.

Columns in the Adapters table

The Adapters table contains the following columns in the default display. You can modify the columns in the default table display by using the **Configure Options** icon or action.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Crypto Number
Indicates the adjunct processor number that is assigned to this adapter. This number is associated with the use of the Adjunct Processor Extended Addressing (APXA) facility, which is only available on specific systems. This facility increases the number of usage domains that can be supported on one cryptographic adapter.

Conflicts
Displays a warning icon in the column, only if one or more domain conflicts exist for a specific adapter. To display additional information about the conflicts, click the warning icon to open the Crypto Conflicts window. For more details, see “Crypto Conflicts - adapter” on page 726.

Type
Indicates the mode in which the cryptographic adapter is configured on this system.

CCA coprocessor
The adapter is configured as a Secure CCA coprocessor (CEX4C) for Federal Information Processing Standard (FIPS) 140-2 Level 4 certification.

EP11 coprocessor
The adapter is configured as an Enterprise PKCS#11 (EP11) coprocessor (CEX4P) for an industry-standardized set of services that adhere to the PKCS #11 specification v2.20 and more recent amendments.

Accelerator
The adapter is configured as an Accelerator (CEX5A) for acceleration of public key and private key cryptographic operations that are used with Secure Sockets Layer/Transport Layer Security (SSL/TLS) processing.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific Crypto Express adapter names.

Location
Provides the location of the adapter in the I/O cage of the system.

Description
Displays the user-provided description, if any, of the adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

The Adapter Domains table toolbar

When you first use the **New Partition** task, the Cryptos display contains only an Adapters table; after you add crypto adapters, the display also includes an Adapter Domains table.

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both.

Add Control Domains
Opens the **Add Control Domains** window through which you can add more control domains. For more information, see the Add Control Domains section in "Adding cryptographic adapters and domains" on page 724.

Add Usage Domains
Opens the **Add Usage Domains** window through which you can add more usage domains. For more information, see the Add Usage Domains section in "Adding cryptographic adapters and domains" on page 724.

Remove
Opens the **Remove Domains** confirmation window through which you can remove one or more domains from the partition definition. This action is enabled when one or more domains are selected in the table.

In the confirmation window, click one of the following buttons:

- Click **Remove** to confirm that you want to remove the selected domains. The confirmation window closes, and the resulting Adapter Domains table display does not contain any entries for the deleted domains.
- Click **Cancel** to close the confirmation window and return to the Cryptos section, without removing any domains.

Columns in the Adapter Domains table

The Adapter Domains table lists each selected usage or control domain in a table row, with a table column for each of the selected adapters that are associated with the domain. Depending on how many adapters you selected, you might need to use the horizontal scroll controls to see all of the table columns.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

Domain Index
Displays the index number assigned to each of the usage domains or control domains added to the partition definition. A letter icon that precedes the index number indicates whether the domain is a usage domain (**U**) or a control domain (**C**).

Adapters
Each remaining column in the Adapter Domains table represents a selected adapter, with the adapter name shown as the column heading. For each domain listed in the table, the adapter column displays either a checkmark or a warning icon, to indicate whether any conflicts exist. To display additional information about the conflict, click the warning icon to display the Crypto Conflicts window. For more details, see "Crypto Conflicts - Usage Domain number" on page 727.

Standard table functions

In addition to the customized action icons and the Actions list, the Adapters table and Adapter Domains table toolbars include the following standard table functions.

Configure Options
Provides a way to exclude or include specific columns from the table display. Select this option from the **Actions** list or click the Configure Options icon (). Available columns are listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Advanced Filter
Provides advanced filter options through which you can reduce the total number of table entries. To access filter options, click the Filter icon ().

Adding cryptographic adapters and domains

When you first select **Add** to add cryptographic adapters to the partition definition, DPM opens a dialog that consists of several windows through which you can select adapters and domains. On any window, you can click **Cancel** to close the dialog and return to the Cryptos section. Otherwise, make a selection and click **OK** to advance to the next window.

In contrast, when you subsequently access the dialog windows through selections in the **Actions** list of the Adapter Domains table, you can access the domain dialog windows separately; DPM opens the appropriate dialog window, based on your selection. Clicking **OK** or **Cancel** returns you to the Crypto section.

The following lists describe the contents of each dialog window, in the order in which DPM presents them. Each window contains a table through which you make your selections; each of these tables has a toolbar with standard table functions, such as filters.

Add Adapters
The **Add Adapters** window displays a table containing one entry for each available crypto adapter that is not already assigned to this new partition. Use the Select column to select one or more adapters for the new partition to use.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

To select all rows in the table, select the check box in the Select column header. To remove selection from all rows when all rows are selected, clear the check box in the Select column header. To remove the selection from all rows when only some rows are selected, select the check box in the Select column header, and then select it again to clear it.

Name
Displays the name of the adapter. The name is a hyperlink through which you can open the **Adapter Details** task. Alternatively, you can select the adapter in this table, and use the Actions list in the table toolbar to open the **Adapter Details** task.

If this adapter might cause the partition to enter the Degraded state, a warning icon is displayed to the left of the name. To display the state of the adapter, hover your cursor over the warning icon.

Crypto Number
Indicates the adjunct processor number that is assigned to this adapter. This number is associated with the use of the Adjunct Processor Extended Addressing (APXA) facility, which is only available on specific systems. This facility increases the number of usage domains that can be supported on one cryptographic adapter.

Conflicts
Displays a warning icon in the column, only if one or more domain conflicts exist for a specific adapter. To display additional information about the conflicts, click the warning icon to open the Crypto Conflicts window. For more details, see "Crypto Conflicts - adapter" on page 726.

If you select an adapter that has domain conflicts, a message is displayed above the table:

- If the partition is active or if you have selected the **Reserve resources** check box in the General section, the message reports an error. In this case, you must select a different adapter.
- If you have not selected the **Reserve resources** check box, the message is only a warning that your new partition might not be successfully started because at least one other partition definition contains the same adapter and usage domain.

Type
Indicates the mode in which the cryptographic adapter is configured on this system.

CCA coprocessor
The adapter is configured as a Secure CCA coprocessor (CEX4C) for Federal Information Processing Standard (FIPS) 140-2 Level 4 certification.

EP11 coprocessor
The adapter is configured as an Enterprise PKCS#11 (EP11) coprocessor (CEX4P) for an industry-standardized set of services that adhere to the PKCS #11 specification v2.20 and more recent amendments.

Accelerator
The adapter is configured as an Accelerator (CEX5A) for acceleration of public key and private key cryptographic operations that are used with Secure Sockets Layer/Transport Layer Security (SSL/TLS) processing.

Card Type
Indicates the type of adapter card, which varies depending on the adapter cards that the system supports. Valid values include specific Crypto Express adapter names.

Utilization
Indicates the average utilization for the adapter over the last five minutes. If the percentage is high (for example, 90%), consider selecting a different adapter. The utilization is shown in both a graphic progress bar and in numeric percentage.

Usage Domain Allocation
Indicates the percentage of usage domains that are currently allocated to this adapter. If the percentage is high (for example, 90%), consider selecting a different adapter. The percentage is shown in both a graphic progress bar and in numeric format. The displayed percentage includes usage domains only for started and reserved partitions. To display this numeric percentage along with the numeric percentage for all partitions, hover your cursor over the column cell. The percentage for all partitions cannot exceed 100%.

Each adapter supports up to 16 usage domains, but that limit can be increased through the use of the adjunct processor extended addressing facility, depending on the machine type and configuration of the DPM-enabled system. If you select an adapter that does not have sufficient allocation space, an error message is displayed above the table, indicating that the new partition might fail to start because this adapter does not have sufficient allocation space.

Location
Provides the location of the adapter in the I/O cage of the system.

Description
Displays the user-provided description, if any, of the adapter. To edit the existing text or provide a description, double-click in the table cell and type the new description. The description can be up to 1024 characters in length.

Add Usage Domains
The **Add Usage Domains** window displays a table containing one entry that represents each available usage domain and control domain, with usage domains listed first, by default. To limit the table entries to only those domains that are not defined to any partition on the system, select the **Hide usage domains defined to other partitions** check box. By default, the check box is checked.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

Domain Index
Indicates the index number assigned to the usage domain or control domain. Each coprocessor or accelerator contains a specific number of usage domains, identified by an index number, which contain an isolated set of master keys. When you create a new partition, you select only one usage domain index to assign to your partition, and that index assignment applies for each cryptographic adapter that your partition can access. If you select a control domain, it is converted into a usage domain.

Conflicts
When the **Hide usage domains defined to other partitions** check box is unchecked, the Conflicts column is shown in the table. If a conflict exists for a specific domain, a warning icon is shown in the column. To display additional information about the conflict, click the warning icon to display the Crypto Conflicts window. For more details, see "Crypto Conflicts - Usage Domain number" on page 727.

If you select a domain that has conflicts, a message is displayed above the table:

- If the partition is active or if you have selected the **Reserve resources** check box in the General section, the message reports an error. In this case, you must select a different usage domain.
- If you have not selected the **Reserve resources** check box, the message is only a warning that your new partition might not be successfully started because at least one other partition definition contains the usage domain for one or more of the same adapters.

Add Control Domains
The **Add Control Domain** window displays a table containing one entry that represents each available control domain.

Select
Enables the selection of table entries. No rows are selected when the table is first displayed. You can select one or more table entries.

Domain Index
Indicates the index number assigned to the control domain. Control domains provide only the ability to manage domains and keys. If the partition is configured as the TCP/IP host for the Trusted Key Entry (TKE) workstation, you need to assign control domain indexes to the partition. Otherwise, selecting a control domain is optional. You can select one or more control domains.

Crypto Conflicts - adapter

Use the Crypto Conflicts window to view details about domain conflicts for a specific adapter, the name of which is displayed in the window title. This window contains the Conflicting Partitions table, which contains an entry for each partition for which the definition includes the same cryptographic adapter and usage domains that you have selected for the new partition. The table contains the following columns.

Partition
Displays the name of a partition for which the definition contains one or more adapters or domains that match those you have selected for the new partition. The name is a hyperlink through which you can open the **Partition Details** task.

Active/Reserved
Indicates whether the existing partition is active or reserved. If the partition is either active or reserved, a checkmark is displayed.

Usage Domains
Specifies each of the domain index numbers that conflict with those index numbers you have selected for the new partition. If multiple index numbers are in conflict, each number is separated by a comma; if consecutive index numbers are in conflict, they are shown in ranges. For example: `0-3, 5, 8-10`

To close the window and return to the previous window, click **Close**.

Crypto Conflicts - Usage Domain number

Use the Crypto Conflicts window to view details about the conflicts for a specific usage domain, the index number of which is displayed in the window title. This window contains the Conflicting Partitions table, which contains an entry for each partition for which the definition includes the same usage domain for one or more cryptographic adapters that you have selected for the new partition. The table contains the following columns.

Partition
Displays the name of a partition for which the definition contains one or more adapters or domains that match those you have selected for the new partition. The name is a hyperlink through which you can open the **Partition Details** task.

Active/Reserved
Indicates whether the existing partition is active or reserved. If the partition is either active or reserved, a checkmark is displayed.

Adapters (Crypto Number)
Displays the name of each adapter that is associated with the usage domain. The name includes the crypto number, which is shown in parentheses. Each adapter name is a hyperlink through which you can open the **Adapter Details** task. If multiple adapters are listed for a specific partition, each adapter is shown on a separate line in the table.

To close the window and return to the previous window, click **Close**.

Partition links

Use the **Partition links** section to view the partition links, if any, that interconnect this partition with one or more other partitions. If no partition links are defined yet, you can use links in this section to open the **Configure Partition Links** task to the overview page. You can view, create, edit, or delete partition links through the **Configure Partition Links** task only.

If partition links are defined, the Partition links table contains a row for each existing partition link that is attached to this partition, with the following information.

Name
Specifies the name of the partition link. The partition link name must be unique for a given system. The name is a hyperlink through which you can open the **Configure Partition Links** to the details page for the specific partition link.

Link state
Specifies the current state of the partition link. Note that the partition link state does not affect the partition state of any partitions to which the link is attached.

Complete
The partition link is attached to at least two partitions.

Incomplete
The partition link is attached to fewer than two partitions.

Updating
As the result of a create, edit, or delete request, processing is pending or ongoing. For example, when you create a partition link, DPM asynchronously attaches the partition link to the partitions that you added as part of the create request. This attachment process might take some time, depending on the status and number of the added partitions. The attachment to stopped

partitions is relatively quick, but attachment to active partitions can take longer because driving dynamic I/O updates takes some time.

Note: You cannot edit or delete a partition link that is in Updating state.

Link type
Specifies the type of partition link: SMC-D (Shared Memory Communications - Direct Memory Access)

Partitions
Specifies the number of the partitions to which this link is attached.

Description
The user-supplied description, if any. Descriptions can consist of a maximum of 200 characters.

Boot

Partitions on a DPM-enabled system can host a single operating system or hypervisor. Use the Boot section to view the currently selected option, or to select the location of the executables for the hypervisor or operating system to be run in this partition, or to upload the required files to initialize the hypervisor or operating system when the partition itself is started. Some of these boot options require that you find and select an ISO image file, which is a collection of files and metadata for installing software, and an .INS file, which maps image components (for example, kernel, ramdisk, parameter file) to the appropriate storage addresses in main memory.

To modify boot options, complete the following steps.

1. Click the down arrow to display the available options in the "Boot from" menu.
2. Choose one of the available options and provide any additional information that is required. For a detailed explanation of each boot option, plus instructions for providing required information, see “Boot from menu options” on page 728.

   When you select a specific boot option, the display shows editable fields and other information related to the selected option.
3. Review the **Boot loader time-out** setting and, if necessary, change it. By default, the time-out setting for most boot options has a value of 60 seconds. For only the **Network server (PXE)** boot option, the default time-out setting is 600 seconds, to account for network traffic. If the boot loader takes longer than the time-out value to load the hypervisor or operating system executables, DPM cancels the operation and issues an error message.
4. When you have finished, review another section or click **OK** to save the partition definition.

For the supported boot options and more detailed instructions for installing z/VM in a partition, see the *IBM Dynamic Partition Manager Guide*, which is available on IBM Documentation at https://www.ibm.com/docs/en/systems-hardware

"Boot from" menu options

The "Boot from" menu lists the boot options that are available for the hypervisor or operating system. If an option in the list is disabled, hover your cursor over that option to display additional information for that option. If necessary, take appropriate action to make that selection available; for example, if you want to use the Storage device (SAN) option, return to the Storage page to attach a storage group with a boot volume.

Secure Service Container
This boot option is the default for a Secure Service Container partition. The display includes the Boot in Installer Mode switch, which determines what processing is done when you start the partition.

YES
With the switch set to **YES**, the partition start process initializes the Secure Service Container Installer so you can install an appliance in the partition.

NO
With the switch set to **NO**, the partition start process effectively restarts an installed appliance. In this case, the Secure Service Container Installer is rebooted, and the installed appliance is

restarted in the Secure Service Container partition on this and all subsequent reboots, until you change the switch setting.

Storage Group (SAN) or Storage device (SAN)

Select this option when the hypervisor or operating system executables reside on an internal or external storage device. This option is available only when storage groups or host bus adapters (HBAs) are defined for the partition.

When you select this option, the Boot section contains either a Storage Groups table or an HBA table. The Storage Groups table is displayed only when the DPM R3.1 storage management feature or a later DPM version is applied on the system. Follow the instructions that correspond to the type of table displayed on the page.

- "Boot from a boot volume in a storage group" on page 729 (only for systems with the DPM R3.1 storage management feature or a later DPM version applied)

  Note: Starting with DPM R4.0, you can select options to validate the operating system image that you boot from a volume in a storage group. For more information, see "Secure Boot options" on page 733.
- "Boot from a boot volume accessed through an HBA" on page 730

Boot from a boot volume in a storage group

The Storage Groups table displays the available storage groups that contain a boot volume. To view the available boot volumes, expand any table entry by selecting the storage group. The Storage Group table contains the following columns.

Select
Use a radio button in the Select column to identify the storage group that contains the boot volume for the operating system or hypervisor. Depending on the fulfillment state of the storage group and availability of a boot volume, the radio button might be disabled.

Name
Specifies the user-defined name of the storage group.

Type
Specifies the type of storage group: FICON, FCP, or NVMe. The expanded table display contains a Boot Volume table that lists all available boot volumes that the storage group contains. The Boot Volume table content and Advanced Boot Volume Settings fields vary, depending on the storage group type.

- For each boot volume in an FCP storage group, the Boot Volume table provides the universally unique identifier (UUID) and capacity of the volume, along with a user-supplied description, if any.
- For each boot volume in a FICON storage group, the Boot Volume table provides the name of the storage subsystem in which the volume resides, along with the volume ID, capacity, type, and device number. If a user-supplied description is available, it is also displayed in the table.

  If you select a boot volume in a FICON storage group, the Boot page display also includes an expandable section called Boot loader settings, where you can select the type of boot loader: List-directed or Channel Command Word (CCW). Select the option that matches the formatting type of the operating system image on the boot volume. You cannot select CCW when the **Secure Boot** check box is selected.
- For each boot volume in an NVMe storage group, the Boot Volume table provides the boot volume serial number and capacity, along with a user-supplied description, if any. When you select an NVMe volume, note that NVMe namespace management is not supported, so you can boot programs only from namespace ID=1.
- For descriptions of the optional fields in the Advanced Boot Volume Settings area, see Advanced (optional) boot settings.

Partitions
Specifies the number of partitions to which the storage group is attached.

Shareable
Specifies whether the storage group can be shared among partitions, or whether it is dedicated to only one partition.

Total Capacity
Specifies the total amount of storage in gibibytes (GiBs) that is assigned to the storage group.

Description
Specifies the user-provided description, if any, of this storage group.

Fulfillment state

Checking migration
This fulfillment state indicates that DPM is checking the logical and physical elements that support a storage group it created during a system migration or firmware upgrade process.

Complete
The storage group is ready for use.

Incomplete
One or more volumes or adapters that are used for a storage group are marked as incomplete. DPM periodically checks the availability of storage volumes or adapters for storage groups, so resources that were functioning properly can become incomplete.

Pending
A system administrator has sent a request to create or modify a FICON or FCP storage group, but the storage administrator has not finished fulfilling that request through tools for managing storage subsystems.

Pending with mismatches
For an FCP storage group, a system administrator sent a request to create or modify that storage group, and the storage administrator fulfilled that request, but with an amount of storage that does not exactly match the original request. For an NVMe storage group, as part of a repair, one or more NVMe SSDs were replaced with SSDs of a different size.

Boot from a boot volume accessed through an HBA

The HBA table displays the available host bus adapters. Select the HBA connected to the storage subsystem that hosts the boot volume, provide the 64-bit worldwide port number (WWPN) of the storage subsystem, and provide the 64-bit hexadecimal logical unit number (LUN) of the volume that contains the boot image. For example:

Target WWPN: `50:0a:09:85:87:09:68:ad` or `500a0985870968` (hexadecimal)
Target LUN: `4021400000000000`

Advanced (optional) boot settings

In addition, you can provide values for the following optional fields. The optional fields in the display vary, depending on whether you selected an HBA, an NVMe storage group, an FCP storage group, or a FICON storage group. If you selected a storage group, the optional fields are displayed under the list of boot volumes in the expanded table entry for the storage group.

Boot program selector (0-30)
The boot program selector is a single number that identifies a boot configuration on the SAN device, which can contain up to 31 (decimal 0 – 30) different configurations. Each configuration can be a Linux kernel, a kernel parameter file, or optionally a ram disk. Configurations are prepared through the Linux zipl tool.

The default is the **Automatic** option, but specifying a value can be useful for backup purposes.

Boot record location
The default is the **Use volume label** option. If you select **Specific value**, enter hexadecimal values for the cylinder, head, and record to identify the boot record location on the boot volume.

Boot record logical block address
The boot record logical block address identifies the entry or anchor point where the boot loader can find the hypervisor or operating system. For Linux operating systems, this address is the master boot record and is usually the first block on the IPL device. Through this optional setting, you can provide a different block address as the entry point. If you provide a value, specify the 64-bit load block address as a 16-digit hexadecimal string.

IPL load parameter
This optional field can contain initial program load (IPL) parameters to be passed to the operating system or hypervisor. You can specify a maximum of eight alphanumeric characters.

OS load parameters
Through this optional setting, you can provide operating system-specific parameters to be passed to the hypervisor or operating system during SCSI IPL (initial program load). The hypervisor or operating system has to support load parameters being passed during IPL.

For a Linux operating system, use this field to specify kernel parameters. During the boot process, these parameters are concatenated to the end of the existing kernel parameters that are used by your boot configuration.

- The specifications must contain ASCII characters only. If characters other than ASCII are present, the content of the field is ignored during IPL.
- If you specify the kernel parameters with a leading equal sign (=), the existing kernel parameters are ignored and replaced with the kernel parameters in this field.
- If you replace the existing kernel parameters, be sure not to omit any kernel parameters required by your boot configuration.

You can also specify load parameters to log in to the operating system or hypervisor through either the **Operating System Messages** task or the **Integrated 3270 Console** task:

- For the **Operating System Messages** task, type `sysc`
- For the **Integrated 3270 Console** task, type `sysg`

Network server (PXE)
Select this option when you want to use a preboot execution environment (PXE) on a network server. This option is available only if a network interface card (NIC) for either an OSA port or HiperSockets switch is defined for the partition.

When you select this option, the NIC table displays the available network interface cards. Select the NIC for the adapter that connects the partition to the network on which the network boot server resides.

FTP server
Select this option if you want to use FTP to boot an image that is located on a different system. Provide the following information:

Host name
Enter either the fully qualified domain name of the FTP server, or its IP address.

User name
Enter the user name on the target FTP server.

Password
Enter the password associated with the user name on the target FTP server.

INS file
Either click **Browse** to retrieve a list of INS files from the target FTP server and select one file, or enter the fully qualified name (relative to FTP root) of an INS file.

Depending on the size of the FTP site, browsing might require more time than manually entering the full path and name of the INS file. Also note that the browsing function returns INS files found in the user's home directory or its subdirectories. Because you cannot select a starting directory, or navigate to a directory above the user's home directory, manually entering the full path and name of the INS file might be more expedient.

If you click **Browse**, a separate window displays the user's home directory and its subdirectories. Select one INS file, and click **OK** to close the Browse FTP Server window.

FTPS server
Select this option if you want to use the FTP Secure (FTPS) protocol to boot an image that is located on a different system. FTPS uses the Secure Socket Layer (SSL) protocol to secure data. With this option, you need to supply a host name, user ID, password, and .INS file, as described for the **FTP server** boot option.

SFTP server
Select this option if you want to use the Secure File Transfer Protocol (SFTP) to boot an image that is located on a different system. SFTP uses the Secure Shell (SSH) protocol to secure data. With this option, you need to supply a host name, user ID, password, and .INS file, as described for the **FTP server** boot option.

Hardware Management Console removable media
Select this option if you want to use an INS file from a media drive that is connected to the HMC. The media drive must be installed in the HMC when you save the partition definition and when the partition is started. Possible drive selections are **CD/DVD drive** or **USB flash memory drive**, depending on what media drives are installed in the HMC. If an option is displayed but is not selectable, an inline message or tool tip explains why the selection is disabled.

If the partition is configured to boot from a CD/DVD drive and the HMC that you are using does not have a CD/DVD drive installed, you might be required to change the drive selection.

- If the **CD/DVD drive** selection was configured on a different HMC that is still available for managing partitions and still has a CD/DVD drive installed, you do not have to change this boot option. In this case, you can continue to boot the partition from the other HMC. However, if you do change the boot option, you cannot reselect the **CD/DVD drive** selection through this HMC.
- If the **CD/DVD drive** selection was configured on the HMC that you are currently using, and this HMC no longer has a CD/DVD drive installed, you must change the boot option for this partition.

When you select this option:

1. If more than one type of media drive is available on the HMC, select the radio button for the media drive on which the INS file resides. Otherwise, skip to the next step.
2. Either enter the fully qualified name (relative to the mount point) of an INS file, or complete the following steps.
   a. Select **Browse** to start a search on the target media drive to retrieve a list of INS files. Any INS files found are displayed in a separate window.
   b. Select only one INS file and click **OK** to close the Browse Removable Media window.

ISO image
Select this option when you want to upload an ISO file that is located on your workstation file system. This option is available only when you are connecting to the HMC through a remote browser.

When you select this option:

1. Select **Browse** to find the ISO image file on your workstation file system. You cannot select an ISO image from an HMC media drive. As soon as you select an ISO image file, DPM starts to upload the file, and displays a progress indicator for the upload operation.
2. After the upload operation completes, click **Browse** to search the ISO image file for the INS file that you want to use. Any INS files found are displayed in a separate window. Select only one INS file and click **OK** to close the Browse ISO Image window.

None
Select this option if you want to start a partition without a hypervisor or operating system. Although the partition can be started, it is not in a usable state.

Secure Boot options

Secure Boot options enable DPM to validate that the Linux operating system executables on a boot volume originate from a trusted source, and have not been altered without authorization. The Boot page display includes the **Secure Boot** check box, which is not enabled until:

- You select the **Storage Group (SAN)** option in the "Boot from" menu.
- The system and partition meet specific requirements that vary, depending on the DPM release.

DPM R4.0 to R5.0

With these releases, DPM verifies that the software signature matches the signature from the distributor, using trusted public keys that reside in the hardware and are identical for all partitions and systems. If the signatures do not match, the boot process fails.

This option is enabled only when:

- The partition has a partition type of **Linux**.
- The system that hosts the partition supports the IBM Secure Execution for Linux function.
- You are booting the Linux operating system from a volume in an FCP or NVMe storage group.

DPM R5.1

With this release, DPM validates the digital signature of the operating system image using the public cryptographic keys that are contained in customer-supplied digital certificates from the Linux distributor. A security administrator can import digital certificates and manage them through the **Secure Boot Certificate Management** task.

Note: If you have already used the hardware public keys for a specific partition (the Secure Boot option available with DPM R4.0-R5.0), DPM continues to use those hardware keys until you assign one or more digital certificates to the partition; after that certificate assignment, for this partition only, the hardware keys are no longer valid.

This option is enabled only when:

- The partition has a partition type of **Linux** or **z/VM**. Note, however, that for a partition with the **z/VM** type, the certificates apply only when booting the Linux guests, not when booting the z/VM hypervisor itself.
- You are booting the Linux operating system from a volume in an FCP, FICON, or NVMe storage group.

The Boot section contains a Certificates table that lists the certificates, if any, that a security administrator has imported for use on the system. When the **Secure Boot** check box is selected:

- Depending on your authorization, you can use the Certificates table to assign one or more certificates to the partition, or you can select **Manage** to open the **Secure Boot Certificate Management** task to import certificates to use. If any certificates in the table are already selected (the check box contains a check mark), those certificates are already assigned to this partition. You can change which certificates are selected by modifying the Certificates table entries or, with the appropriate authority, through the **Secure Boot Certificate Management** task.
- You must assign one or more certificates before the partition is started. If DPM does not find at least one matching certificate when the partition is started, the boot process fails and the partition status changes to Terminated and then to Stopped. If the image to be booted contains multiple signed components that require individual certificates, all of the required certificates must be assigned for the boot process to succeed.
- The boot process fails if one or more of the required certificates have expired. The suggested practice is to replace or remove expired certificates. Periodic hardware messages indicate when a certificate is approaching or has passed its expiration date.
- If you assign or unassign certificates while a partition is active, the changes do not take effect until the boot process is run again (that is, when the partition is stopped and restarted or when the operating system is rebooted).
- If you select a boot volume in a FICON storage group, the display also includes an expandable section called Boot loader settings, directly under the **Secure Boot** check box. Because the Channel

Command Word (CCW) is the standard boot loader type, it is the default setting. However, when the **Secure Boot** check box is selected, the List-directed boot loader type is automatically selected and cannot be changed. The List-directed setting provides audit records that can help you diagnose a failure due to a signature mismatch. Note that the List-directed boot loader type requires that installer programs support a specific image format on the boot volume.

Also, more advanced boot settings are displayed under the boot volume information in the Storage Groups table; these settings vary depending on the type of storage group that contains the boot volume. (Descriptions of the advanced boot settings are in the **Storage Group (SAN)** section in "Boot from menu options" on page 728.)

Confirm Disruptive Action Dialog

Use the **Confirm Disruptive Action** dialog to confirm that you want to make the changes that you specified in a section of the **Partition Details** task, even though this partition is not stopped.

This dialog is displayed for one of the following requests:

- A request to change the device number, virtual LAN (VLAN) ID, or media access control (MAC) address of one or more network interface cards (NICs).
- A request to change the device number of one or more host bus adapters (HBAs) or virtual functions (VFs).
- A request to change the adapter or adapter port of one or more NICs, HBAs, or VFs.
- A request to delete one or more NICs, HBAs, or VFs.
- A request to remove one or more crypto adapters, usage domains, or control domains.
- A request to change the current login or network settings for a Secure Service Container partition.

Depending on the type of requested changes, you might be required to type in confirmation text or enter your password. On the **Confirm Disruptive Action** dialog, complete the following steps.

1. Review the Changes table to verify the disruptive changes that you requested. This table contains the following columns:

   Name
   Contains one of the following values:
   - The name of a NIC, HBA, or VF
   - The name of a crypto adapter
   - The number of the usage domain or control domain
   - Reset Login for a change to the master user ID or password for a Secure Service Container partition
   - Reset Network for a change to the values for the Secure Service Container Web Interface Communication

   Type
   Contains one of the following values:
   - NIC
   - HBA
   - VF
   - Crypto Adapter
   - Crypto Usage Domain
   - Crypto Control Domain
   - Secure Service Container

   Change
   Contains additional text to describe the requested disruptive change.

2. Review the Partition table to determine whether you must type a confirmation value. This table contains the following columns:

   Name
   The name of the partition for which you are requesting disruptive changes.

   System
   The system that is associated with this partition. The system name is a hyperlink through which you can open the **System Details** task.

   Status
   The current status of this partition.

   OS Name
   The operating system name that is associated with this partition.

   Confirmation Text
   This column is displayed only if you are required to type in confirmation that the action will disrupt a partition's operations. To confirm, type either the value in the Name column, or the value in the OS Name column, exactly as it is displayed in this table.
3. If you are required to enter a password, this display includes a text box in which you need to type the password associated with your user ID.
4. Click **Save** to save the changes that you have requested, or click **Cancel** to close the window without saving any changes.

Perform a Repair Action

Accessing the Perform a Repair Action task

Note: You cannot perform this task remotely.

This task should be the starting point for all repairs. You can either repair an open problem or report a repair of a non-detected problem.

To start a repair action:

1. Open the **Perform a Repair Action** task. The Perform a Repair Action window is displayed.
   - To start a repair or continue a repair of a previously reported problem, select **Manage open problems**.
   - To report about repairing a problem that was not detected or reported by Problem Analysis, select **Report a repair of a non-detected failure**.
2. Click **NEXT** to start the repair.

Perform a Repair Action

Use this window to either:

- Repair an open problem
- Resume a delayed repair
- Report the repair of a problem that was not detected or reported by Problem Analysis.

Use this window to select the type of repair action you want to perform:

Manage open problems
To repair an open problem, or to resume a delayed repair, select **Manage open problem**.

Additional repair support (Open FRU)
For additional repair support and proceed through that process, select **Additional repair support (Open FRU)**.

Report a repair of a non-detected failure
To report information about repairing a problem that was not detected or reported by Problem Analysis, select **Report a repair of a non-detected failure**.

Additional functions on this window include:

NEXT
To continue the task after selecting the type of repair action you want to take, click **NEXT**.

CANCEL
To close this window and cancel the task, click **CANCEL**.

Display Open Problems

Use this window to select a problem to work on and to select the work you want to do.

Select a problem to work on from the "Problem Report table" on page 737, then select a choice from the menu bar.

You can work with the table by using the table icons or **Select Action** list from the table toolbar. If you place your cursor over an icon, the icon description is displayed. The icons and list actions perform the following functions:

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want. Click **OK** when you have defined your filter. The filtered view can be toggled on and off by selecting the check box next to the desired filter in the filter row. If you no longer want the **Filter** row to appear, click **Hide Filter Row**.

Clear All Filters
Returns to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header to change from ascending to descending order. Click **OK** when you have defined your preferred order.

Clear All Sorts
Returns the table back to the default order.

Configure Columns
Allows you to arrange the columns in the table in the order you want or to hide columns from view. All available columns are listed in the Columns list by their column names. You select the columns you want displayed or hidden by selecting or clearing the box next to the column names. Manipulate the column order by selecting a column name in the list and clicking the arrows to the right of the list to change the order of the selected columns. When you have completed the configuration and you want to save the settings, click **OK**. Otherwise, click **Cancel** and your changes will not be saved.

Click **Select Action** on the menu bar then select the following:

- **Problem** to list problems by order of problem numbers, from the highest number to the lowest number.
- **Timestamp** to list problems in order of the dates on which they occurred, from the most recent problem to the least recent problem.
- **SRC** to list problems by alphanumeric order of reference codes.
- **Status** to list problems by order of their priority for repair. Delayed problems are listed first, followed by open problems, followed by any remaining problems.

Click **Manage problems** on the menu bar to select the following:

- Repair Selected Problem to start a repair procedure for the selected problem.
- **Close selected problem** to change the status of the selected problem to closed.

- **Close all problems** to change the status of all problems to closed.

Click **View** on the menu bar to select the following:

- **Problem Analysis Panels** to display again the panels Problem Analysis displayed to report the selected problem when it occurred.
- Problem Summary to display additional information that further describes the selected problem, and lists actions performed to diagnose and correct the problem.
- **Refresh** to update the list with recently opened problems.
- **Exit** to close this window and return to the previous window.

Problem Report table

Problems to work on are listed in this table. Select a problem, then use the menu bar choices to select the work you want to do.

Problem
Displays the problem number assigned by Problem Analysis when the problem was detected, and used to identify and track the problem.

Timestamp
Displays the date and time the problem occurred.

SRC
Identifies the specific error condition associated with the problem.

Status
Indicates whether the problem is open, delayed, or otherwise worked on.

Problem FRU List

This window displays the location and part number or parts that you may need to replace to repair the problem.

You can work with the table by using the table icon or **Select Action** list from the table toolbar. If you place your cursor over the icon, the icon description is displayed. The icon and list action perform the following function:

Configure Columns
Allows you to arrange the columns in the table in the order you want or to hide columns from view. All available columns are listed in the Columns list by their column names. You select the columns you want displayed or hidden by selecting or clearing the box next to the column names. Manipulate the column order by selecting a column name in the list and clicking the arrows to the right of the list to change the order of the selected columns. When you have completed the configuration and you want to save the settings, click **OK**. Otherwise, click **Cancel** and your changes will not be saved.

The window also identifies the printed documentation you need to use to repair the problem.

Location
Displays the physical location of the part in the hardware configuration.

Part number
Displays the Custom Card Identification Number (CCIN) of the part.

Make note of any field replaceable units listed to refer to when using the printed documentation.

Additional functions from the **Action** drop-down list include:

Continue after completing all actions in documentation
To confirm you have completed using printed documentation to repair the problem, select **Continue after completing all actions in documentation**.

Delay the repair
To close this window while you use printed documentation to repair the problem, select **Delay the repair**.

Cancel the repair
To close this window and cancel the repair, select **Cancel the repair**.

View Problem Analysis Panels
To display again the panels Problem Analysis displayed to report the selected problem when it occurred, select **View Problem Analysis Panels**.

Report a Repair of an Unreported Problem

Use this window to identify the outcome of work you performed to repair a problem that was not detected or reported by Problem Analysis.

Select whether or not parts were exchanged as a result of the repair, then click **NEXT**.

Yes, FRUs were exchanged to fix the failure
To indicate you exchanged parts to repair the problem, select **Yes, FRUs were exchanged to fix the failure**.

Note: At least one of the exchanged parts must be in the hardware configuration of this Hardware Management Console.

No, FRUs were not exchanged to fix the failure
To indicate you did not exchange parts to repair the problem, select **No, FRUs were not exchanged to fix the failure**.

Note: Select this choice also if you exchanged parts, but all exchanged parts were outside the hardware configuration of this Hardware Management Console.

Additional functions on this window include:

NEXT
To continue the task after you make a selection, click **NEXT**.

CANCEL
To close this window and cancel the task, click **CANCEL**.

Continued Repair from Documentation

Use this window to identify the outcome of work you performed using printed documentation to repair a problem.

Select one choice for the repair action, then click **NEXT**.

Yes, FRUs exchanged to fix the failure
To indicate you exchanged parts to repair the problem, select **Yes, FRUs exchanged to fix the failure**.

Note: At least one of the exchanged parts must be in the hardware configuration of this Hardware Management Console.

No, FRUs were not exchanged to fix the failure
To indicate you did not exchange parts to repair the problem, select **No, FRUs were not exchanged to fix the failure**.

Note: Select this choice also if you exchanged parts, but all exchanged parts were outside the hardware configuration of this Hardware Management Console.

A new problem was detected
To indicate a new problem occurred while you were repairing the current problem, select **A new problem was detected**.

The status of current problem will become delayed. Repair the new problem before resuming repair of the delayed problem.

Additional functions on this window include:

NEXT
To continue the task after you make a selection, click **NEXT**.

CANCEL
To close this window and cancel the task, click **CANCEL**.

Enter Repair Description

Use this window to specify a description of the work you performed to repair a problem.

NEXT
To continue the task after specifying a description of the repair action, click **NEXT**.

Problem Summary

This window displays additional information that describes the selected problem.

System name
Displays the name of the object on which the problem occurred

Machine type
Displays the machine type of the object

Machine model
Displays the model number of the object

Machine serial
Displays the serial number of the object.

Remote support problem number
Displays the number assigned to the problem by the support system

Additional functions on this window include:

NEXT
To continue the task after you complete this window, click **NEXT**.

Perform Model Conversion

Accessing the Perform Model Conversion task

Use this task to add, remove, or update system hardware and features. Some system configuration tasks support performing system upgrades and model conversions. Follow your normal order process for ordering an upgrade or model conversion for your system.

Note: When the power save mode is active some upgrade options are not available for the **Perform Model Conversion** task. See the **Set Power Saving** task.

To add, remove, or update system hardware and features:

1. Open the **Perform Model Conversion** task.

   The Perform Model Conversion window lists the upgrades and features for your system.
2. Select the perform model conversion option you want to work with.

Hardware Upgrades
Select this option to add memory or processor drawer upgrades to hardware on your system.

Permanent upgrades
Select this option to order permanent capacity upgrades to processors, memory, and the Crypto Assist Feature (CAF) to your system. Retrieve your upgrade data from the support system or from a media source.

Temporary upgrades
Select this option to temporarily increase, add, or replace processor capacity on your system. Retrieve, install, and activated tasks for temporary records (On/Off CoD, CBU, or Planned Event) are all separate records located on the support system or media device.

Feature on Demand
Select this option to display information on all installed features on your system and information on the features contained in the staged record on the system. You can apply all the features contained in the staged record or permanently remove the staged record from the system.

Features
Select this option to add or remove available features on your system.

Perform Model Conversion

Use this window to add, remove or update system hardware and features.

Is it recommended that if new hardware is associated with the model upgrade then it should be installed prior to executing selections from this window. It is required that this function be initiated after Standby power-on. It is also recommended (but not required) that this function be initiated prior to system power on.

Hardware upgrades
Select this option to add hardware upgrades to your system.

Add processor drawer hardware
Select this option to add additional processor drawer hardware to your system.

Fanout card Rebalance
Select this option to move current Fanout card locations to available Fanout card locations.

“Prepare for Enhanced Processor Drawer Availability” on page 742
Select this option to prepare your system for Enhanced Processor Drawer Availability on a targeted processor drawer. This option is a prerequisite to the Perform Enhanced Processor Drawer Availability option and determines the readiness of the system for the targeted processor drawer.

“Perform Enhanced Processor Drawer Availability Results” on page 743
Select this option to concurrently perform the Enhanced Processor Drawer Availability on the targeted processor drawer that was previously prepared.

“Display Previous Prepare for Enhanced Processor Drawer Availability Results” on page 745
Select this option to view the results from the last execution of the Prepare for Enhanced Processor Drawer Availability.

System Anchor Record (SAR) upgrade data from media
Select this option to retrieve and apply system anchor record data from a media source.

Add I/O Processor Drawer
Select this option to add a hardware I/O processor drawer to your system.

Remove I/O Processor Drawer
Select this option to remove a hardware I/O processor drawer from your system.

Permanent upgrades
The permanent upgrades allow you to order permanent capacity upgrades to processors and memory without disrupting application already running on your system. You have the choice to retrieve and apply from the support system or from a media source.

Retrieve and apply
Select an option to retrieve and apply a permanent upgrade from the support system or a media source.

Processor/memory upgrade data from support system
Select this option to retrieve and apply permanent upgrade data from the support system.

Processor/memory upgrade data from media
Select this option to retrieve and apply permanent upgrade data from a media source.

Retrieve processor/memory upgrade data but do not apply
Select this option to retrieve permanent upgrade data from the support system, but do not apply the upgrade at this time.

Apply processor/memory upgrade data (previously retrieved)
Select this option to apply permanent processor/memory upgrade data to your system that was previously retrieved.

“Display Processor Upgrade Data” on page 746
Select this option to display the current permanent processor configuration on the system. Staged processor data displays if there is a permanent record staged on the system.

Remove processor/memory upgrade data (previously retrieved)
Select this option to remove previously retrieved permanent LICCC upgrade data that was not yet installed.

Retrieve and apply channel upgrade
Select this option to retrieve and apply a permanent channel upgrade if any channel card is being upgraded without hardware replacement. If any channel card is being upgraded without replacing hardware, special processing is required which includes handling of the diskette that was shipped for this purpose.

Perform pre-check on media upgrade
Select this option to perform a pre-check on the requested permanent configuration upgrade and any active temporary upgrades presently on the system that would prevent the requested permanent upgrade from being installed.

“Temporary upgrades” on page 748
The temporary upgrades allows you to temporarily increase, add, or replace processor capacity on your system. Retrieve, install, and activated tasks for temporary records (On/Off CoD, CBU, Planned Event, or Loaner Engine) are all separate records located on the support system or media device. Up to 8 records can be installed at any given time. You can have one On/Off CoD record installed or activated at any given time.

Retrieve
Select an option to retrieve temporary upgrade data (On/Off CoD, CBU, Planned Event, or Loaner Engine) from the support system or a media source.

Processor upgrade data from support system
Select this option to retrieve a temporary upgrade from the support system.

Processor upgrade data from media
Select this option to retrieve a temporary upgrade from a media source.

Manage
Select this option to manage all of the temporary installed records and staged records on your system.

View
Select this option to view all of the temporary installed records on your system.

History
Select this option to view the history of all actions performed on all temporary upgrades.

“Feature on Demand” on page 755
Select an option to retrieve and apply or not apply FoD data from media, installed features, and features contained in the staged record on your system.

Retrieve and Apply FoD data from media
Select this option to retrieve and apply FoD data from media.

Retrieve FoD data but do not apply
Select this option to retrieve FoD data from media but do not apply.

Manage
Select an option to manage installed or staged record features on your system:

Installed
Displays information on all the installed features on your system.

Staged
Displays information on the features contained in the staged record on the system.

“Features” on page 756
Select an option to add or remove available features on your system.

“Add a Feature” on page 756
Select this option to install features to your system from a removable media device. To install the features on your system, insert the removable media device into your Support Element and select the media you are using to install the features.

Note: If you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message is displayed indicating the drive was not added and that you should remove the device and try again.

“Remove a Feature” on page 756
Select this option to display all features available for your system and the option to remove installed features.

Additional functions on this window include:

Cancel
To close the window without making a selection, click **Cancel.**

Help
To display help for the current window, click **Help**.

Prepare for Enhanced Processor Drawer Availability

Use this option to prepare the system for Enhanced Processor Drawer Availability on a targeted processor drawer. This option is a prerequisite to the Perform Enhanced Processor Drawer Availability option and determines the readiness of the system for the targeted processor drawer. The configured processors and the in-use memory will be evaluated for evacuation from the targeted processor drawer to the unused resources available on the remaining processor drawers within the system configuration. In addition the I/O connections associated with the targeted processor drawer will be analyzed for any Single Path I/O connectivity.

There are three states which can result from the prepare option:

- The system is ready to perform the Enhanced Processor Drawer Availability for the targeted processor drawer within the original configuration.
- The system is not ready to perform the Enhanced Processor Drawer Availability because of conditions specified from the Prepare for Enhanced Processor Drawer Availability option. For more details see System not ready to Perform Enhanced Book Availability
- The system is ready to perform the Enhanced Processor Drawer Availability for the targeted processor drawer. However, processors may need to be reassigned from the original configuration in order to continue. For more details see the Reassign Non-Dedicated Processors

Select the targeted processor drawer to be upgraded from the selection table:

Processor Drawer
Displays the available processor drawers installed in your system

Location
Displays the physical location of the processor drawer on your system

Additional functions on this window include:

OK
To perform or prepare an enhance Processor Drawer Availability option, click **OK**.

Cancel
To close the window without making a selection, click **Cancel.**

Help
To display help for the current window, click **Help**.

Perform Enhanced Processor Drawer Availability Results

Use this option to concurrently perform the Enhanced Processor Drawer Availability on the targeted processor drawer that was previously prepared. This option allows for the evacuation of system resources from the targeted processor drawer, removal of the processor drawer, removal of memory hardware, addition of new memory hardware, reinstallation of the targeted processor drawer, and finally the restoration of the targeted processor drawer into the system configuration. A graphical interface will guide you with all hardware manipulations.

System not ready to Perform Enhanced Processor Drawer Availability

Use this window to review the conditions that are preventing the Enhanced Processor Drawer Availability option from being performed. There are tabs on the window for Processors, Memory, and for various Single Path I/O conditions. Only the tabs that have conditions preventing the perform option from being executed will be displayed. Each tab indicates what the specific conditions are and possible options to correct the conditions. The following list are possible conditions that may need to be corrected:

Additional functions on this window include:

OK
To perform or prepare an enhance Processor Drawer Availability option, click **OK**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Processors

Use this window to view the corrective actions required for the processor configuration conditions that are preventing the Perform Enhanced Processor Drawer Availability option from being performed for the targeted processor drawer.

Note: You may need to deactivate partitions or deconfigure processors to meet requirements as indicated by the window data.

Use the following table as a guide to meet your system requirements.

Dedicated PUs
Displays the number of dedicated processing units in your system

Shared CPs
Displays the number of shared central processors defined in your system

Shared ICFs
Displays the number of shared internal coupling facility processors defined in your system

Shared zIIPs
Displays the number of shared z integrated information processors defined in your system

Partition Name
Displays the name of the logical partitions defined in your system.

Memory

Use this window to view the corrective actions required for the memory configuration conditions that are preventing the Perform Enhanced Processor Drawer Availability option from being performed for the targeted processor drawer. The In-Use memory must be less than or equal to the available memory on the remaining processor drawers within the system.

Note: You may need to deactivate partitions to meet requirements as indicated by the window data.

In-use memory
Displays the amount of physical memory that is being used on your system.

Available memory
Displays the amount of memory remaining on your system.

Use the following table to view the in-use memory installed on your system.

In-use memory
Displays the amount of physical memory in-use on your system

Partition Name
Displays the name of the active logical partition on your system.

Single Path I/O

Use this window to view the corrective actions required for the single I/O, single domain I/O, or single alternate I/O configuration conditions that are preventing the Perform Enhanced Processor Drawer Availability option from being performed for the targeted processor drawer.

Notes:

- For the single I/O conditions, you will need to deconfigure all of the PCHIDs that are indicated by the window data.
- For the single domain I/O conditions, you will need to change the alternate path to a different processor drawer or deconfigure the PCHID.
- For the single alternate I/O conditions, you will need to correct the alternate path error conditions or deconfigure the PCHIDs.

Use the following table to review the PCHID(s) on your system that need to be deconfigured.

PCHID
Displays a four-digit physical channel identifier of each channel path

CSS
Displays a single-digit number that identifies the channel subsystem

CHPID
Displays a two-digit number that is a channel path identifier of each channel path

Partition Name
Displays the names of the logical partitions defined in your system.

Reassign Non-Dedicated Processors

Use this window to change or accept the system processor assignments that are generated during the processing of the Prepare for Enhanced Processor Drawer Availability option. The processor values that are entered from this window will be the processor configuration utilized during the Perform Enhanced Processor Drawer Availability processing.

Attention: The values should never be altered without approval from your system programmer.

Use this table to view the physical processor assignments in your system to reassign.

Processor Type
Displays the physical processors assigned to the logical partitions logical processors

Non-Dedicated Count
Displays the number of non-dedicated processors in each logical partition's logical processors assignment

Dedicated Count
Displays the number of dedicated processors in each logical partition's logical processor assignment.

Processor Totals
Displays the total amount of physical processors installed in your system.

LICCC
Displays the amount of licensed internal code installed in your system

Additional functions on this window include:

OK
To return to the previous window, click **OK**.

Cancel
To close the window without making a selection, click **Cancel.**

Help
To display help for the current window, click **Help**.

Processor Assignments Panel

Use this window to view the system processor assignments that are generated during the processing of the Prepare for Enhanced Processor Drawer Availability option. The processor values that are displayed from this window are the processor configuration utilized during the Perform Enhanced Processor Drawer Availability processing.

Use this table to view the physical processor assignments in your system.

Processor Type
Displays the physical processors assigned to the logical partitions logical processors

Dedicated Count
Displays the number of dedicated processors in each logical partition's logical processor assignment.

Non-Dedicated Count
Displays the number of non-dedicated processors in each logical partition's logical processors assignment

Processor Totals
Displays the total amount of physical processors installed in your system.

LICCC Count
Displays the number of processors which licensed internal code has been applied.

Additional functions on this window include:

Cancel
To close the window without making a selection, click **Cancel.**

Help
To display help for the current window, click **Help**.

Display Previous Prepare for Enhanced Processor Drawer Availability Results

Use this option to view the results from the last execution of the Prepare for Enhanced Processor Drawer Availability option.

Additional functions on this window include:

OK
To return to the previous window, click**OK**.

Help
To display help for the current window, click **Help**.

Disruptive I/O Remove

Use this window to remove an I/O cage and/or hardware processor drawer disruptively from your system. You can work with the table by using the table icons or **Select Action** from the table tool bar. If you place your cursor over an icon, the icon description appears. The icons perform the following functions:

Selecting Rows
You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block. Click **Select All** or **Deselect All** to select or deselect all objects in the table.

Configure column
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the

list box and using the arrow buttons to the right of the list to change the order of the selected column. When you have completed the configuration, click **OK**. The columns appear in the table as you specified.

Additional functions on this window include:

OK
To perform the disruptive operation and remove the selected I/O cage and/or processor drawer to be removed from your system, click **OK**.

Help
To display help for the current window, click **Help**.

Display Processor Upgrade Data

The window displays the current installed permanent processor configuration on the system and any staged processor data if there is a permanent record staged on the system.

Order #
Displays the order number for this permanent upgrade. This applies to CIU records only. This field is blank for records that are not retrieved through CIU.

Memory (GB)
Displays the amount of LICCC enabled memory.

Crypto Assist Feature
Displays YES if the Crypto Assist feature is enabled.

CPs
Displays the number of CPs that are LICCC enabled.

Additional functions on this window include:

OK
To return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Active/Unassigned

The window displays the current installed permanent processors that are active and unassigned on your system.

SAPs
Displays the active/unassigned system assist processors installed on your system.

ICFs
Displays the active/unassigned internal coupling facility processors installed on your system

IFLs
Displays the active/unassigned integrated facility for Linux processors installed on your system.

zIIPs
Displays the active/unassigned z integrated information processors installed on your system.

Active/Maximum

The window displays the MSU value and model-capacity identifier for the current installed permanent processors.

MSU
Displays the permanent MSU value.

Model-Capacity Identifier
Displays the permanent model-capacity identifier.

Customer Initiated Upgrade Order Activation Number

Use this window to enter the order activation number provided to activate a Customer Initiated Upgrade.

- Type your **Order activation number** here. The **Order activation number** is a number supplied which activates the Customer Initiated Upgrade.

Additional functions on this window include:

OK
To save the changes you made, click **OK**.

Cancel
To close the window without making a selection, click **Cancel.**

Help
To display help for the current window, click **Help**.

Select Customer Initiated Upgrade(s)

Use this window to retrieve, apply, remove or view the status of the CIU feature data. The CIU upgrade data that can be retrieved and applied includes CIU upgrades, On/Off CoD upgrades, and may also include CBU upgrades.

The upgrades can be done individually or in any combination. Go to Resource Link at www.ibm.com/servers/resourcelink to order the upgrades prior to applying them.

Under most circumstances all CIU orders can be concurrently applied to the system. However, there are times when this is not possible and the upgrade must be applied disruptively. If an upgrade is disruptive (requiring a power-on reset), a message is displayed on the support element allowing you the option to apply the upgrade at a more convenient time.

Select one of the possible actions related to customer initiated upgrades, then click **OK**.

Retrieve and apply upgrades
Use this selection to retrieve CIU upgrade data from the support system and activate the upgrade.

Retrieve upgrade data but do not apply
Use this selection to only retrieve the CIU upgrade data from the support system with the option to apply it at a later time. The upgrade data will be saved on the system until it is applied or removed. The data may also be viewed while residing on the system.

This option should not be used when activating a CIU order for On/Off CoD. If you select **Retrieve upgrade data but do not apply** and an On/Off CoD order was retrieved from the support system, you are given the option to apply the upgrade now. If you do not select to apply data now, then the data is removed from the system and you will need to retrieve and apply the On/Off CoD order at a later time.

Apply previously retrieved upgrades
Use this selection to apply previously retrieved CIU upgrade data from the support system. The On/Off CoD upgrade is not supported.

View upgrades
Use this selection to display the current CIU upgrade data that was previously retrieved from the support system but not yet applied.

Remove upgrades
Use this selection to remove upgrade data that was previously obtained using the **Retrieve upgrade data but do not apply** selection. You may select any combination of upgrades that you want removed. Once removed, you will no longer be able to apply the selected upgrades.

Note: The CIU **Remove upgrades** option is only available in the service representative mode.

Additional functions on this window include:

OK
To save the changes you made, click **OK**.

Cancel
To close the window without making a selection, click **Cancel.**

Help
To display help for the current window, click **Help**.

Remove Customer Initiated Upgrade Selections

Use this window to select any combination of previously obtained upgrades that you want removed. Once removed, the selected upgrades will no longer be available. You can contact your support system if you need assistance. You can select any combination of upgrades to be removed. This includes processor drawer upgrades, capacity backup features, or both.

Select the check box(es) to indicate which upgrades to remove. You can choose **Processor Drawer upgrade**, **Capacity backup feature**, or both.

Additional functions on this window include:

OK
To remove the selected upgrades from the current order number, click **OK**.

Cancel
To close the window without making a selection, click **Cancel.**

Help
To display help for the current window, click **Help**.

Temporary upgrades

The window displays the selected installed records and any staged records available for the temporary processor upgrades to your system.

- Installed records include information on the current state of all the installed temporary upgrades on your system. Review the information under **Installed Records**. Optionally, click **Details**, **Add processors**, **Remove processors**, or **Delete** to change the temporary installed upgrades on your system.
- Staged records include information on temporary upgrades retrieved from the support system or selected media. The staged records window requires moving temporary upgrades to the installed area when there is availability of less than 8 installed upgrades. Review the information under **Staged Records**. Optionally, click **Details**, **Install**, or **Delete** to change the temporary staged upgrades on your system.

There are several different types of temporary upgrades:

- On/Off CoD
- CBU
- Boost
- Flex Capacity
- Flex On/Off CoD

There can be up to a total of 8 capacity upgrades active on the system at the same time, with the exception that among those 8 there can only be one billing capacity upgrade at a time. The capacity upgrades can be combined with up to 7 replacement capacity upgrades.

Additional functions on this window include:

Cancel
To close the window without making a selection, click **Cancel.**

Installed records

The window displays the current state of all the installed upgrades on your system.

Note: Pending processor counts indicate the number of processors pending activation when the hardware becomes available. Pending processors will become active as soon as resources become available

(adding hardware or removing other temporary records). Pending CLIs indicate the number of capacity level increases pending activation. Pending CLIs become active as soon as other temporary records which increased the capacity level are deactivated.

Record ID
Displays the ID uniquely identifying the record on the system.

Record type
Displays the type of upgrade this record is used for (On/Off CoD, CBU, Planned event).

CLIs
Displays the maximum/pending/active capacity level changes for each record.

CPs
Displays the maximum/pending/active general purpose processors installed for each record.

SAPs
Displays the maximum/pending/active system assist processors installed for each record.

ICFs
Displays the maximum/pending/active internal coupling facility processors installed for each record.

IFLs
Displays the maximum/pending/active integrated facility for Linux processors installed for each record.

zIIPs
Displays the maximum/pending/active z integrated information processors installed for each record.

Status
Displays the state of the record: (installed, active, staged, or expired) for each record. Check the hardware message for additional details. If Attention displays, hovering the mouse over the record will display one of the following:

- out of activations
- out of activation days for one or more processor types
- low on activation days for one or more processor types
- record has expired
- record is going to expire soon
- out of activation days for the record
- low on activation days for the record

Status details
Displays status details if the status field displays **Attention**.

Additional functions on this window include:

Details...
To display details of a selected record, click **Details...**.

Add processors...(manage mode only)
To open the Change Activation Levels window and add (activate) processors to a selected record, click **Add processors...**.

Remove processors...(manage mode only)
To open the Change Activation Levels window and remove (deactivate) processors from a selected record, click **Remove processors...**.

Delete (manage mode only)
To delete a selected record permanently from the system, click **Delete**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Status details

The Status details displays information why the installed record is in the attention state. The attention state details displays one of the following:

No activations remaining
There are no activations left for this record. For Capacity Backup (CBU), the real and possibly test activations need to be replenished. For Capacity for Planned Events (CPE), the record should be removed and another one ordered. You can also contact your service representative for more information.

No processor/MSU days remaining
There are no days remaining for either one or more processors, MSUs, or both.

Few processor/MSU days remaining
There are 5 or fewer days remaining for either one or more processors, MSUs, or both.

Record is expired
The record has exceeded its expiration date.

Record is about to expire
The record will reach its expiration date in 5 or fewer days.

No activation days remaining
There are no activation days remaining.

Few activation days remaining
There are 5 or fewer activation days remaining.

System summary

The system summary information displays the following:

Model capacity-identifier
Displays the overall model-capacity identifier resulting from the permanent LICCC values and all the active temporary records.

Model temporary-capacity identifier
This is determined using the permanent LICCC values and the activation levels of the billable temporary capacity records.

Model permanent-capacity identifier
This is determined using the permanent LICCC values.

MSUs
Displays the billable MSU value.

Available PUs
Displays the number of remaining PUs available for activation.

Record details

The window displays details for a selected installed upgrade, and allows you to add and/or remove processors on your system. Each section represents the maximum values as well as the resources that are active or remaining. There are different types of records with different limits that apply to them. There are some fields that do not apply to all records and will be indicated as such.

Record ID
Displays the ID uniquely identifying this selected record on the system.

Record Type
Displays the type of upgrade this selected record is used for (On/Off CoD, CBU, CBU (pre-paid), Planned event).

Status details
Displays status details if the status field displays **Attention**.

Activation Time
If this record is active, this field displays the date and time it was activated.

Description
Displays a description of this selected record. The description is initially set when the order is made, but can be changed at any time after installing the record.

Original Description
Displays the original description that this selected record came with when it was ordered.

Status
Displays the state of this selected record: (installed, active, staged, or expired).

Displays the state of the record: (installed, active, staged, or expired) for each record. Check the hardware message for additional details. If Attention displays, hovering the mouse over the record will display one of the following:

- out of activations
- out of activation days for one or more processor types
- low on activation days for one or more processor types
- record has expired
- record is going to expire soon
- out of activation days for the record
- low on activation days for the record

CIU order #
Displays the order number for this selected record upgrade. This only applies to CIU records. For records that are not retrieved through CIU, this field is blank.

User
Displays the last user who acted on this selected record.

Additional functions on this window include:

OK
To exit this window and return to the previous window, click **OK**.

Add processors...(manage mode only)
To open the Change Activation Levels window and add (activate) processors to a selected record, click **Add processors...**.

Remove processors...(manage mode only)
To open the Change Activation Levels window and remove (deactivate) processors from a selected record, click **Remove processors...**.

Update description (manage mode only)
To change or update a description you entered for a selected record in the Description entry field, click **Update description**.

Set as default CBU (manage mode only)
To activate or deactivate all the resources in the default CBU record, click **Set as Default CBU**. If there is no default CBU record specified, the oldest CBU record is used.

Refresh
To display updated changes, click **Refresh**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Resources

The resource limits section information displays the following:

Model-capacity identifier
Displays the maximum/current model-capacity identifier for the system.

Maximum MSU percentage
Displays the maximum MSU percentage for the system.

Resource Counts table
Displays the maximum/pending/active values for each processor.

Pending resource counts indicate the number of processors or capacity level increases pending activation when the hardware becomes available. Pending resources will become active as soon as resources become available (adding hardware or removing other temporary records).

Capacity pools (Remaining/Consumption Rate)

The capacity pools section information displays the following:

Processor Tokens
Displays the number of tokens remaining for each processor.

MSU Tokens
Displays the number of MSU tokens remaining for this selected record.

Real Activations
Displays the number of real activations remaining for this selected record.

Test Activations
Displays the number of test activations remaining for this selected record.

Time limits

The time limits section information displays the following:

Record Expiration Date
Displays the date that this selected record expires.

Real Activation Hours Remaining
Displays the number of hours remaining for a real activation for this selected record.

Test Activation Hours Remaining
Displays the number of hours remaining for a test activation for this selected record.

Change activation levels

The window displays all the information necessary to activate or deactivate an accounting record.

Record ID
Displays the ID uniquely identifying this selected record on the system.

Description
Displays a description of this selected record. The description is initially set when the order is made, but can be changed at any time after installing the record.

Status details
Displays status details if the status field displays **Attention**.

Status
Displays the state of the selected record: (installed, active, staged, or expired) for each record. Check the hardware message for additional details. If Attention displays, hovering the mouse over the record will display one of the following:

- out of activations
- out of activation days for one or more processor types
- low on activation days for one or more processor types
- record has expired
- record is going to expire soon
- out of activation days for the record
- low on activation days for the record

Model-Capacity table
Displays all possible target model-capacity identifiers that can be activated or deactivated with this selected record.

You can work with the table by using the table icons or **Select Action** from the table tool bar. If you place your cursor over an icon, the icon description appears. The icons perform the following functions:

Show filter row
Displays a row under the title row of the table. Select **Filter** found under a column title to define a filter for that column. This limits the entries in the table. Tables can be filtered to show only those entries most important to you. Click **OK** when you have defined your filter. The filtered view can be toggled on and off by selecting the check box next to the desired filter in the filter row. If you no longer want the **Filter** row to appear, click **Hide Filter Row**.

Clear all filters
Returns the table back to the complete listing.

Edit sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **OK** when you have defined your preferred order.

Clear all sorts
Returns the table back to the default order.

Configure column
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column. When you have completed the configuration, click **OK**. The columns appear in the table as you specified.

Additional functions on this window include:

OK
When all changes are complete and you want to update the selected record with current changes, click **OK**.

Cancel
To exit this window and return to the previous window, click **Cancel**.

Restore Current Levels
To restore this selected record level that was activated to the previous current record level, click **Restore Current Levels** then click **OK**.

Undo
To restore this selected record level that was activated prior to the first time the selected record was activated, click **Undo** then click **OK**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Processors

The processors section allows counts for each processor type to be changed according to the LICCC data for this selected record. The current value is displayed to the right of the drop down boxes.

Note: The total number of used processing units cannot exceed the total number of physically available processing units. If the LICCC value is greater than the available processing unit count, the maximum value in each processor drop down box is the available processing units, not the LICCC value.

Activation options

The activation options only display for selected records that allow test activation. If this section is visible, the activation can be either real or test.

Note: If a record is already activated for test, it must be deactivated prior to activating it for real and vice versa. If a record is activated for test or real, this section will display, but is disabled until the record is deactivated.

Upgrade history

The window displays a history of all upgrades performed on your system.

Date and Time
Displays the data and time an action was performed on the selected record.

Record ID
Displays the record ID uniquely identifying the selected record on the system.

Action
Displays one of the following actions performed for the selected record:

Activate
Displays when the activation levels were changed for the selected record.

Deactivate
Displays when the activation levels were changed for the selected record.

Expired
Displays when the activation levels expired for the selected record.

Install
Displays when the selected record was moved from the staged area to the installed area.

Replenish
Displays when the selected record was replenished.

Delete
Displays when the selected record was permanently removed from the system.

Permanent
Displays when a change was made to the Permanent LICCC on the system.

The history is initially sorted by the date and time the changes were made to the selected records. You can work with the table by using the table icons or **Select Action** from the table tool bar. If you place your cursor over an icon, the icon description appears. The icons perform the following functions:

Show filter row
Displays a row under the title row of the table. Select **Filter** found under a column title to define a filter for that column. This limits the entries in the table. Tables can be filtered to show only those entries most important to you. Click **OK** when you have defined your filter. The filtered view can be toggled on and off by selecting the check box next to the desired filter in the filter row. If you no longer want the **Filter** row to appear, click **Hide Filter Row**.

Clear all filters
Returns the table back to the complete listing.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **OK** when you have defined your preferred order.

Clear all sorts
Returns the table back to the default order.

Configure column
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column. When you have completed the configuration, click **OK**. The columns appear in the table as you specified.

Additional functions are available from this window:

Details...
To display details for the selected record, click **Details...**.

Cancel
To exit this window and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Staged records

The window displays the selected records that were retrieved from the support system or selected media that requires moving to the installed area when there is the availability of less than 8 installed upgrades.

Additional functions are available from this window:

Details...
To open the selected Record Details window, click **Details...**.

Install (manage mode only)
To add the selected record to an available install slot (manage mode only), click **Install**.

Delete (manage mode only)
To permanently remove the selected stage record from the system (manage mode only), click **Delete**.

Help
To display help for the current window, click **Help**.

Feature on Demand

The window displays the installed features on the system and features contained in the staged record.

- Installed displays information on all the installed features on your system. Review the information under **Installed**. Optionally, use the table icons or **Select Action** from the table tool bar to permanently remove features from your system.
- Staged displays information on the features contained in the staged record on the system. Review the information under **Staged**. Optionally, click **Apply Record** to apply ALL the features contained in the staged record to the system or click **Remove Record** to permanently remove the staged record from the system.

Additional functions are available from this window:

Cancel
To close this window and exit this option, click **Cancel**.

Help
To display help for the current window, click **Help**.

Installed

This page displays the current installed features on your system and an option to permanently remove any installed features.

You can work with the table by using the table icons or **Select Action** from the table tool bar.

Remove Feature
Removes the selected installed feature permanently from your system.

If you place your cursor over an icon, the icon description appears. The icons perform the following functions:

Configure Columns
Selects which columns you want to display. Arrange the columns in the table in the order you want or hide columns from view. All available columns are displayed in the **Columns** list by their column name. You select the columns you want to display or hide by selecting or clearing the items in the list and using the arrows to the right of the list to change the order of the selected column. When you have

completed the configuration, click **OK**. The columns are displayed in the table as you specified. Your configuration changes are saved and reloaded the next time that you launch this task.

Staged

The page displays the features contained in the staged record and an option to apply ALL the features in the staged record or permanently remove the record from the system. There can only be one record staged at any given time.

Apply Record
To apply ALL the features contained in the staged record to the system, click **Apply Record**.

Remove Record
To permanently remove the staged feature from the system, click **Remove Record**.

Features

This option allows you to add or remove features installed and supported for your.

- "Add a Feature" on page 756 displays a list of one or more features you can install on your system.
- "Remove a Feature" on page 756 displays all features supported on your system and allows you to remove installed features.

Additional functions are available from this window:

Cancel
To close this window and exit this option, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add a Feature

This window allows you to select one or more of the features you want to install on your system that were on the removable media device. Select the one or more of the listed features you want to install then click **OK**.

OK
To perform the operation, click **OK**.

Cancel
To close the window without making a selection, click **Cancel**.

Help
To display help for the current window, click **Help**.

Remove a Feature

This window displays all features supported for your system and allows you to remove installed features on your system. The features currently installed on your system are indicated by "Currently Active" next to them. Select the one or more of the listed features you want to remove then click **OK**.

OK
To perform the operation, click **OK**.

Help
To display help for the current window, click **Help**.

Perform Problem Analysis

Accessing the Perform Problem Analysis task

The Support Element starts Problem Analysis automatically only upon detecting a problem. While the Support Element provides very comprehensive error detection, if it does not detect a problem you suspect is affecting the system or Support Element, you can use the Support Element workplace to start Problem Analysis manually.

To start Problem Analysis manually:

1. Locate the system to work with.
2. Open the **Perform Problem Analysis** task.
3. Use the Perform Problem Analysis window to start Problem Analysis manually.

   Problem Analysis will issue a hardware message to notify you if it identifies a problem.
4. Click **View All Errors...** to view details on all error in the display list.
5. Click **View Selected Errors...** to view details on a selected error in the display list.
6. Click **Cancel** to exit the window.

Accessing the View Service History task

You can use the Support Element workplace to display the service history of the system. This task displays a list of current problems for the system. The problems may be opened or closed with the most recent entry at the top of the list.

To display the service history:

1. Locate the system to work with.
2. From the menu bar you can:
   - Select **View** for the following choices:

     Problem Summary
     Displays detailed information about the selected problem including machine type, model, and serial number information.

     Problem Analysis Panels
     Redisplays the Problem Analysis (PA) windows that were created when the selected problem was originally reported.

     Repair Information
     Displays repair information for the selected problem.

     Exit
     Ends the task.
   - Select **Close** for the following choices:

     Selected Problem
     Changes the current status of the selected problem to closed.

     All Problems
     Changes the current status of all open problems to closed.
   - Select **Sort** for the following choices:

     By Date
     Lists problems in the order of the dates on which problems occurred, starting with the most recent problem.

     By System Name
     Lists problems by the alphabetical order of the names of the objects on which they occurred.

     By Status
     Lists all open problems, followed by all closed problems.
   - Select **Help** to display additional task information.
3. When you have completed this task, select **View**, **Exit**.

Service History

Use this window to review or close problems discovered by Problem Analysis, or reported using Problem Analysis, for one or more objects.

A problem is *opened* when either:

- Problem Analysis determines service is required to correct a problem detected by the object
- A console operator uses the **Report a Problem** task to report a suspected problem not detected by the object.

Each record of a problem includes detailed information about the problem, and indicates whether the service required to correct the problem is still pending (an *opened* problem), or is already completed or no longer needed (a *closed* problem).

Collectively, the problem and service records are referred to as the *service history* of the object. Upon viewing the object's service history, you can:

- Redisplay the Problem Analysis windows that were displayed when a problem was originally reported.
- Display detailed information about a problem.
- Manually close open problems.

Click **View** on the menu bar, then select the following:

- **Problem Summary...** to display additional information that further describes the selected problem and the object it occurred on, and lists actions performed to diagnose and correct the problem.
- **Problem Analysis Panels...** to display Problem Analysis panels that were shown to report the selected problem when it occurred.
- **Repair Information...** to display the repair information for the selected problem.
- **Exit** to end this task and return to the console workplace.

Click **Close** on the menu bar, then select the following:

- **Selected Problem** to change the status of selected *open* problems to *closed*.
- **All Problems** to change the status of all *open* problems to *closed*.

Click **Sort** on the menu bar, then select the following:

- **By Date** to list problems in order of the dates on which they occurred, from the most recent problem to the oldest problem.
- **By System Name** to list problems in alphabetical order of the names of the objects on which they occurred.
- **By Status** to list all *open* problems, followed by all *closed* problems.

Click **Help** to display help for the current window.

Service History table

This list displays the most recent problems that were automatically detected by Problem Analysis, or reported manually using Problem Analysis, for all selected objects.

Date
Displays the date on which the problem occurred.

Time
Displays the time when the problem occurred.

System name
Displays the name of the object on which the problem occurred.

Problem Number
Displays the number assigned by Problem Analysis and used to identify and track the problem.

Status
Indicates whether the problem is *open* or *closed*.

Description
Displays a brief explanation of the problem.

Service History Problem State

This window displays information that identifies an object, describes a specific problem that occurred on it, and lists actions performed to diagnose and correct the problem.

System name
Displays the name of the object on which the problem occurred.

Machine type
Displays the machine type of the object.

Machine model
Displays the model number of the object.

Machine serial number
Displays the serial number of the object.

Remote support problem number
Displays the remote support problem number.

Problem number
Displays the number assigned to the problem by Problem Analysis.

Problem type
Identifies the type of problem reported to the support system by Problem Analysis, and indicates the type of service required to correct it.

Problem data
Displays additional information provided by Problem Analysis specifically for this problem.

The information may be part numbers of parts needed to repair the problem, or reference codes needed to perform additional problem determination.

Problem State table

Date
Displays the date on which the problem occurred.

Time
Displays the time when the problem occurred.

“Problem States” on page 759
Displays the problem state of the object on which the problem occurred.

Problem States

Descriptions of the problem states or their effects on the problem:

Additional problem information
Indicates a service representative, while performing a repair procedure, manually edited the service history log to further describe the problem or its repair.

Continued in printed information
Indicates a repair procedure instructed a service representative to continue the repair using a printed repair procedure.

Customer notified
Indicates Problem Analysis displayed a panel to report the problem.

Duplicate problem closed
Indicates Problem Analysis closed the problem because it was a duplicate of another open problem.

Inactive problem closed
Indicates Service History closed the problem because of inactivity.

Problem closed
Indicates Problem Analysis could no longer detect the problem after a service representative completed a repair procedure.

Problem closed by the user
Indicates the console operator used the Service History task to close the problem.

Problem detected
Indicates Problem Analysis detected the problem automatically.

Problem reopened
Indicates Problem Analysis detected the problem occurred again after it was repaired and closed.

Repair closed
Indicates a problem was closed when the repair was completed.

Repair ended
Indicates a service representative completed a repair procedure.

Repair resumed
Indicates a service representative started using a previously suspended repair procedure.

Repair started
Indicates a service representative began a repair procedure.

Repair suspended
Indicates a service representative temporarily stopped using a repair procedure before completing the repair.

Returned from printed information
Indicates a service representative resumed using a repair procedure to acknowledge completing a printed repair procedure.

Service authorization complete
Indicates Problem Analysis successfully transmitted problem information and requested service through a Remote Support Facility (RSF) connection to the support system.

Service authorization delayed
Indicates Problem Analysis reported the problem, but the console operator did not request service.

Service authorization failed
Indicates Problem Analysis could not successfully transmit problem information or request service through a Remote Support Facility (RSF) connection to the support system.

Service authorized electronically
Indicates Problem Analysis used the Remote Support Facility (RSF) to connect to the support system to transmit problem information and request service.

Service requested via telephone
Indicates Problem Analysis displayed problem information and instructed the console operator to call a service representative, describe the problem, and request service.

Additional functions are available from this window:

OK

To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Help
To display help for the current window, click **Help**.

Service History Part Replacement

This window displays part replacement information including part descriptions as well as how many parts were replaced.

Part Location
Displays the machine location of the object on which the problem occurred.

Part Number
Displays the actual part number of the object.

Serial Number
Displays the serial number of the object.

Fix description
The description from Service History of how to correct the problem.

OK

to return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Help
To display help for the current window, click **Help**.

Problem Analysis (problem description)

This window displays the following information about a problem discovered by automatic Problem Analysis:

System name
Displays the name of the object on which the problem occurred.

Date
Displays the date on which the problem occurred.

Time
Displays the time when the problem occurred.

Depending on the information that was provided for a problem, the following information could also appear in this window:

Channel path
Displays a four-digit physical channel identifer (PCHID) of the channel on which the error occurred, for example: 0131, 0132, or 0133.

Unit address
Displays the address of the device the channel path was being used to communicate with when, or immediately before, the Interface Control Code (IFCC) occurred.

Tag-in control lines
Displays a two-digit, hexadecimal value that identifies the inbound tags that were active when the IFCC occurred.

Tag-out control lines
Displays a two-digit, hexadecimal value that identifies the outbound tags that were active when the IFCC occurred.

Bus-in data lines
Displays the value on the inbound data lines when the IFCC occurred.

Bus-out data lines
Displays the value on the outbound data lines when the IFCC occurred.

Use the following information to determine whether to request service, then take the appropriate action:

Problem Description
Provides a brief description of the problem.

Corrective Actions
Describes what actions an operator can take to correct the problem.

Impact of Repair
Describes what system resources will be affected.

Additional functions are available from this window:

Request Service...
To request service to correct the problem, click **Request Service...**.

I/O Trace...
To display Input/Output (I/O) trace information, click **I/O Trace...**.

No Service
To handle the problem without requesting service, click **No Service**.

Display Service Information...
To display information about an automatic Problem Analysis operation on an object, click **Display Service Information...**.

Display Sense Data
To display additional specific problem failure information, click **Display Sense Data**.

Detail Problem Description...
To view a more detailed description of the problem, click **Detail Problem Description...**.

Delete
To delete from **Hardware Messages** the message you selected to display this window, and to close this window, click **Delete**.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Tag-in control lines

This field displays a two-digit, hexadecimal value that identifies the inbound tags that were active when an interface control check (IFCC) occurred.

The hexadecimal number represents the values of eight bits:

- The first digit of the hexadecimal number represents the values for bits 0 through 3.
- The second digit of the hexadecimal number represents the values for bits 4 through 7.
- The value for a bit is 1 when its tag-in is active.
- The value for a bit is 0 when its tag-in is not active.

Bit	Tag-In
0	Operational
1	Address
2	Status
3	Select
4	Request
5	Service or Data (see Note)
6	Data or Mark (see Note)
7	Disconnect

Note: The values for bits 5 and 6 indicate whether the following tags-in are active:

```
Bit 5    Bit 6          Data In       Service       Mark
-----    -----          -------       -------       ----
 1        1              On            Off           Off
 1        0              Off           On            Off
```

```
0       1             Off           Off           On
0       0             Off           Off           Off
```

For example, a tag-in value of 86 indicates that Operational In and Data In are both active.

Tag-out control lines

This field displays a two-digit, hexadecimal value that identifies the outbound tags that were active when an interface control check (IFCC) occurred.

The hexadecimal number represents the values of eight bits:

- The first digit of the hexadecimal number represents the values for bits 0 through 3.
- The second digit of the hexadecimal number represents the values for bits 4 through 7.
- The value for a bit is 1 when its tag-out is active.
- The value for a bit is 0 when its tag-out is not active.

Bit	Tag-In
0	Operational
1	Address
2	Select/Hold
3	Data streaming
4	Service
5	Data
6	Suppress
7	Command

For example, a tag-out value of 84 indicates that Operational Out and Data Out are both active.

Problem Analysis (sense data details)

This window displays sense data details and additional problem failure information.

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Help
To display help for the current window, click **Help**.

Problem Analysis (operation/outcome)

This window displays information about an automatic Problem Analysis operation on an object. The information identifies the operation and describes its outcome.

Review the information, then take the appropriate action.

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Delete Message
To delete from **Hardware Messages** the message you selected to display this window, and to close this window, click **Delete Message**.

Cancel
To close this window and keep the message, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (problem information)

This window displays information about a problem discovered by automatic Problem Analysis.

Use the information provided to determine whether to request service, then take the appropriate action.

System name
Displays the name of the object that had the channel path configured on when the IFCC occurred.

Channel path
Displays a four-digit physical channel identifier (PCHID) of the channel on which the error occurred, for example: 0131, 0132, or 0133.

Unit address
Displays the address of the device the channel path was being used to communicate with when, or immediately before, the IFCC occurred.

Tag-in control lines
Displays a two-digit, hexadecimal value that identifies the inbound tags that were active when the IFCC occurred.

Tag-out control lines
Displays a two-digit, hexadecimal value that identifies the outbound tags that were active when the IFCC occurred.

Bus-in data lines
Displays the value on the inbound data lines when the IFCC occurred.

Bus-out data lines
Displays the value on the outbound data lines when the IFCC occurred.

Additional functions are available from this window:

Problem Description
Provides a brief description of the problem.

Corrective Actions
Describes what actions an operator can take to correct the problem.

Request Service...
To request service to correct the problem, click **Request Service...**.

No Service
To handle the problem without requesting service, click **No Service**.

Display Service Information...
To display information about an automatic Problem Analysis operation on an object, click **Display Service Information...**.

Delete Message
To delete from **Hardware Messages** the message you selected to display this window, and to close this window, click **Delete Message**.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (contact)

Use this window to identify a person that can be contacted about the problem, and to specify how to service will be requested.

Provide the following information, then click **Request Service...**:

Customer name
Specify the name of the person that can be contacted about the problem.

Customer phone
Specify the telephone number of the person that can be contacted about the problem.

Transmission Type
Select how to request service, through automatic transmission or manually by telephone.

Select a transmission type, then click **Request Service...**.

Electronic transmission
To automatically transmit the service request and problem information, select **Electronic transmission**.

Voice transmission
To manually request service and report problem information by telephone, select **Voice transmission**.

Note: The telephone number and problem information are provided on a subsequent window.

Additional functions are available from this window:

Request Service...
To authorize service for this problem and initiate the transmission type by electronic or by voice, select click **Request Service...**.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (problem information/contact)

This window displays information about a problem discovered by automatic Problem Analysis. Use this information to request service and describe the problem.

1. Be ready to provide the problem information when you call.
2. Dial the telephone number to speak with a service representative.
3. Request service.
4. Provide the problem information to the service representative.

Request service when:

- Service is required.
- Service may be required, and you have verified all possible causes of the problem do not exist.

It is recommended you do not request service when:

- Service is not required.
- Service may be required, but you have verified one or more possible causes of the problem exist, and you will attempt to correct the problem.

Additional functions are available from this window:

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (action to take)

This window displays information about a problem discovered by automatic Problem Analysis.

Review the information, then take the appropriate action.

Problem Data
Provides specific information about the selected problem.

Parts List

- Part Location - the physical location of the part.
- Part Number - the number of the part.
- Fix Percentage - the percentage of accuracy for correcting the problem.
- Serial Number - the serial number of the part.
- Quantity - the number of parts.

Additional functions are available from this window:

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Delete Message
To delete from **Hardware Messages** the message you selected to display this window, and to close this window, click **Delete Message**.

Cancel
To close this window and keep the message, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (trace information)

This window displays the following interface trace information:

Function
Whenever possible, a description of the operation being performed for each tag displayed and bus sequence is shown under this field; Interface Disconnect, Interface Control Check (IFCC), Recovery-Hung Interface, etc.

In Tags
Indicates the state of each inbound tag. A plus (+) below the line indicates an active state of the line. A period (.) indicates the inactive state of the line.

REQ
Displays the Request In tag line. This raised by a control unit to indicate it needs service to present status or to perform a data transfer operation.

SEL
Displays the Select In tag line. This is the return of Select Out that indicates no control unit captured the Select Out signal.

OP
Displays the Operational In tag line. This normally indicates the selection of a control unit by the channel.

ADR
Displays the Address In tag line. This defines the information on the Bus In lines as the address of the currently selected I/O device.

STA
Displays the Status In tag line. This defines the information on the Bus In lines as status information.

SRV
Displays the Service In tag line. This defines the information on the Bus In lines as data for a read operation. For a write operation, this indicates a control unit request for data.

DAT
Displays the Data In tag line. This defines the information on the Bus In lines as data for a read operation. For a write operation, this signals a request for data.

DIS
Displays the Disconnect In tag line. This signals a control-unit-detected problem.

MKO
Displays the Mark In 0 line. This is used primarily with the bus extension feature to tell the channel that it is working with a reliable control unit.

Bus In
Indicates the hexadecimal value on the Bus In lines.

Out Tags
Indicates the state of each outbound Tag. A plus (+) below the line indicates an active state of the line. A period (.) indicates the inactive state of the line.

OP
Displays the Operational Out tag line. This is used for interlocking. All outbound tag lines except for Suppress Out are significant only as long as this line is active.

ADR
Displays the Address Out tag line. This defines the information on the Bus Out lines as a device address.

SEL
Displays the Select Out tag line. This captured by a control unit or device waiting to operate with the channel. Capturing Select Out and then Raising Operational In begins the connection process.

CMD
Displays the Command Out tag line. This indicates to stop, proceed, stack status, or identify Bus Out data.

SRV
Displays the Service Out tag line. This defines the information on the Bus Out lines as data for a write operation. For a read operation, this indicates the channel accepted the data. In reply to Status In, this indicates the acceptance of status.

DAT
Displays the Data Out tag line. This defines the information on the Bus Out lines as data.

SUP
Displays the Suppress Out tag line. This is used alone or with other lines to:

- Indicate command chaining
- Force status suppression
- Perform a selective reset
- Force data suppression.

Bus Out
Indicates the hexadecimal value on the Bus Out lines.

Elapsed Time (us)
This field contains elapsed time count data. During critical points of the input/output trace, this count data is reset and the field will contain a line of dashes. The next line entry after this reset will contain the elapsed time from the reset state in microseconds, until that interface operation completes. As each interface sequence occurs, its elapsed completion time will add to the running total until the counter is reset again.

Additional functions are available from this window:

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Help
To display help for the current window, click **Help**.

Problem Analysis (ESCON trace information)

This window displays the following ESCON interface trace information:

- **Function** - the function name
- **UA** - the unit address
- **CCW** - Channel Command Word
- **Flg** - Flags
- **Sta** - Status
- **Other fields** - additional fields
- **Time** - the relative time stamp used for comparison
- **Log Data** - additional data.

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Help
To display help for the current window, click **Help**.

Problem Analysis (I/O trace information)

This window displays the following Input/Output (I/O) interface trace information:

In Tags
Indicates the state of each inbound tag. A plus (+) below the line indicates an active state of the line. A period (.) indicates the inactive state of the line.

REQ
Displays the Request In tag line. This raised by a control unit to indicate it needs service to present status or to perform a data transfer operation.

SEL
Displays the Select In tag line. This is the return of Select Out that indicates no control unit captured the Select Out signal.

OP
Displays the Operational In tag line. This normally indicates the selection of a control unit by the channel.

ADR
Displays the Address In tag line. This defines the information on the Bus In lines as the address of the currently selected I/O device.

STA
Displays the Status In tag line. This defines the information on the Bus In lines as status information.

SRV
Displays the Service In tag line. This defines the information on the Bus In lines as data for a read operation. For a write operation, this indicates a control unit request for data.

DAT
Displays the Data In tag line. This defines the information on the Bus In lines as data for a read operation. For a write operation, this signals a request for data.

DIS
Displays the Disconnect In tag line. This signals a control-unit-detected problem.

MKO
Displays the Mark In 0 line. This is used primarily with the bus extension feature to tell the channel that it is working with a reliable control unit.

Bus In
Indicates the hexadecimal value on the Bus In lines.

Out Tags
Indicates the state of each outbound Tag. A plus (+) below the line indicates an active state of the line. A period (.) indicates the inactive state of the line.

OP
Displays the Operational Out tag line. This is used for interlocking. All outbound tag lines except for Suppress Out are significant only as long as this line is active.

ADR
Displays the Address Out tag line. This defines the information on the Bus Out lines as a device address.

SEL
Displays the Select Out tag line. This captured by a control unit or device waiting to operate with the channel. Capturing Select Out and then Raising Operational In begins the connection process.

CMD
Displays the Command Out tag line. This indicates to stop, proceed, stack status, or identify Bus Out data.

SRV
Displays the Service Out tag line. This defines the information on the Bus Out lines as data for a write operation. For a read operation, this indicates the channel accepted the data. In reply to Status In, this indicates the acceptance of status.

DAT
Displays the Data Out tag line. This defines the information on the Bus Out lines as data.

SUP
Displays the Suppress Out tag line. This is used alone or with other lines to:

- Indicate command chaining
- Force status suppression
- Perform a selective reset
- Force data suppression.

Bus Out
Indicates the hexadecimal value on the Bus Out lines.

Misc
Indicated the state of the non-interface type lines defined by flags. A plus (+) below the line indicates an active state of the line. A period (.) indicates the inactive state of the line.

ACT
Displays the I/O interface active flag. This flag indicates that the I/O interface is active. The interface is considered active when select-out is active. The interface is considered inactive when select-out is inactive, when all bus-in signals are inactive (including bus-in-p), and when all tag-in signals are inactive (except request-in).

DX
Displays the parallel data transfer mode flag. This flag is active during a data transfer operation.

SGV
Displays the stop given flag. A PARDX command out was issued.

ICC
Displays the interface control check error flag.

Elapsed Time (us)
This field contains elapsed time count data. During critical points of the input/output trace, this count data is reset and the field will contain a line of dashes. The next line entry after this reset will contain the elapsed time from the reset state in microseconds, until that interface operation completes. As each interface sequence occurs, its elapsed completion time will add to the running total until the counter is reset again.

Additional functions are available from this window:

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Help
To display help for the current window, click **Help**.

Problem Analysis (channel path errors)

This window displays the unreported errors that occurred on a specific channel path of a Central Processor Complex (CPC).

Use this window to select an error when you want to display detailed information from Problem Analysis that describes the error.

Select one error from the list, then click **Analyze Error...** to display details about the error.

System name
Displays the name of the CPC that had the channel path configured on when the error occurred.

Channel path
Displays a four-digit physical channel identifier (PCHID) of the channel on which the error occurred, for example: 0131, 0132, or 0133.

Interface location
Identifies the physical location of the channel card and port that supports the channel path on which the error occurred.

Additional functions are available from this window:

Error table

Date
Displays the date the error occurred.

Time
Displays the time the error occurred.

Description
Displays a brief description of the error.

Analyze Error...
Select an error from the list, then click **Analyze Error...** to display details about the selected error.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (unreported errors)

This window summarizes the unreported errors that occurred on the system. The summary identifies the problem areas where errors occurred, and displays the number of errors that occurred in each area.

Use this window to select a problem area when you want to display more information about the unreported errors that occurred in the area.

Problem areas for a CPC include the processors and its channels paths.

An unreported error is an error that is analyzed, but is not reported by Problem Analysis. Errors are not reported when automatic recovery operations succeed, and when service is not needed for the system to continue operating.

Select a problem area for a system from the list, then click **View Selected Errors...** to display a summary of unreported errors that occurred in that area.Or, you can click **View All Errors...** to display a listing of all the processor and channel errors sorted by **Date Time** within the **Problem Area**.

Beginning time
Displays the time and date when the least recent unreported error occurred.

All unreported errors occurred at or after this time.

Ending time
Displays the time and date when the most recent unreported error occurred.

All unreported errors occurred before or at this time.

Error table

System Name
Displays the name of the system where the unreported errors occurred.

Problem Area
Indicates whether the unreported errors occurred on a processor in the CPC, or on a particular channel path.

Number of Errors
Indicates the number of unreported errors that occurred in the problem area during the time range.

View All Errors...
To view details about all errors shown in the list, click **View All Errors...**.

View Selected Errors...
To view details about one error in the list, click **View Selected Errors...**.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Power Off or Restart

Accessing the Power Off or Restart task

This task enables you to power off or to restart the console.

To power off or restart the console:

1. Open the **Power Off or Restart** task. The Power Off or Restart window is displayed.
2. You can select one of the following:
   - Restart SE console
   - Power off SE console
   - Restart Firmware Services
   - Power off both primary and alternate SE consoles
   - Restart SE console and power cycle the system (available only for SERVICE user IDs with the appropriate system).
   - Block SE console power off and restart requests
3. Click **OK** to perform the selected action or click **Cancel** to return to the Support Element console workplace.

   Note: If there are other users and tasks running, an additional message is displayed allowing you to send a message (initiates the **Console Messenger** task) to alert the user sessions that you intend to shutdown or restart the console.

Power Off or Restart

This window allows you to restart the console or power off the console.

Note: If this task cannot immediately perform the action that you have selected, a notification appears in a message window. You can wait for your action to complete or click **Cancel** in the message window to exit this task.

Restart SE console
To close the console and restart the console, select **Restart SE console**.

Power off SE console
To close the console and power off the hardware, select **Power off SE console**.

To halt the console, select **Power off SE console**. This completely powers off the console, but leaves the power on. To bring the console back up, use **Ctrl-Alt-Delete**.

Restart Firmware Service
To restart the Support Element after a unsuccessful disruptive logical partition dump, select **Restart Firmware Service**.

Power off both the primary and alternate SE consoles
To power off both the primary and alternate Support Elements, select **Power off both the primary and alternate SE consoles**.

Note: This option only appears if there is both a primary and an alternate SE set up and running. Also, this option is not available if you are running this task remotely or the user ID does not have the correct privileges.

Restart SE console and power cycle the system
To power off both the primary and alternate Support Elements and then cycle the system power when necessary, select **Restart console and power cycle the system**.

Note: This option is only available if you have a SERVICE user ID or a user ID that is assigned service roles. Also, it is only applicable for the appropriate systems.

Block SE console power off or restart requests
To block requests for powering off or restarting the console, select **Block SE power off or restart requests**.

Note: This option is only available if you have a SERVICE user ID or a user ID that is assigned service roles.

OK
To proceed with your selection, click **OK**.

Cancel
To exit this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Remote Power Off Setup and Execution for the HMC, SE, and HMA

To enable remote power off at the Hardware Management Console (HMC), Support Element (SE), or Hardware Management Appliance (HMA), use the following steps for each console. Note, each console setup must be done locally and before remote power off is required. Users that have been assigned system programmer or service roles can perform these steps for remote users.

Remote power off setup

- For the HMC:
  1. Log in locally at the HMC, then open the **Customized Console Services** task. The Customize Console Services window is displayed.
  2. On the **Remote power off or restart** option, click **Change...**. The Change Remote Power Off and Restart Settings window is displayed.
  3. To enable the HMC to be powered off or restarted remotely, select **Power off and restart**, then click **OK**.
- For the SE:
  1. Log in locally at the Primary SE, then open the **Customized Console Services** task. The Customize Console Services window is displayed.
  2. On the **Remote power off or restart** option, click **Change...**. The Change Remote Power Off and Restart Settings window is displayed.
  3. To enable the SE to be powered off or restarted remotely, select **Power off and restart**, then click **OK**.
- For the HMA, you need to configure both the HMC and SE settings locally at the HMA.
  - For the HMC:
    1. Log in locally at the HMC on each HMA, then open the **Customized Console Services** task. The Customize Console Services window is displayed.
    2. On the **Remote power off or restart** option, click **Change...**. The Change Remote Power Off and Restart Settings window is displayed.
    3. To enable the HMC to be powered off or restarted remotely, select **Power off and restart**, then click **OK**.
  - For the SE:

1. Log in locally to the Primary SE on the HMA. Use the key sequence of right-click from the desktop to get flux box menu, then select **SE Console**. Single Object Operation cannot be used.
2. When you are logged in to the SE, open the **Customize Console Services** task. The Customize Console Services window is displayed.
3. On the **Remote power off or restart** option, click **Change...**. The Change Remote Power Off and Restart Settings window is displayed.
4. To enable the SE to be powered off or restarted remotely, select **Power off and restart**, then click **OK**.

Remote power off execution

Once the consoles have been enabled to power off remotely, use the following steps to power off the HMC, SE, and HMA when it is required.

- For the HMC:
  1. Use a remote browser to log in to the HMC, then open the **Power Off or Restart** task. The Power off or Restart window is displayed.
  2. To power off the console, select **Power off HMC console**, then click **OK.**
- For the SE:
  1. Use a remote browser to log in to the HMC. Open the **Single Object Operation** task, select an SE, then click **OK**.
  2. Open the **Power Off or Restart** task. The Power off or Restart window is displayed.
  3. To power off the console, select **Power off SE console** and **Power Off both the primary and alternate SEs**, then click **OK.**
- For the HMA, you must first shut down the console on the SE. Then, power off the console for the HMC.

  Note: It must be done in that order.
  1. For the SE:
     a. Use a remote browser to log in to the HMC, which is on the HMA with the primary SE.
        i) Open the **Single Object Operation** task, select an SE, then click **OK**.
        ii) Open the **Power Off or Restart** task. The Power off or Restart window is displayed.
        iii) To power off the console, select **Power off SE console** and **Power Off both the primary and alternate SEs**, then click **OK.**

        Note: This cleanly shuts down both the Primary and Alternate SEs on both HMAs.
  2. For the HMC:
     a. Use a remote browser to log in to the HMC, which is on the HMA.
     b. Open the **Power Off or Restart** task. The Power off or Restart window is displayed.
     c. To power off the console, select **Power off HMC console**, then click **OK.**

        Note: Repeat the previous steps for the HMC on the second HMA.

Power On Reset

Accessing the Power-On Reset task

A power-on reset initializes a system by:

- Initializing all processors.
- Initializing the channel subsystem.
- Allocating storage.
- Loading the hardware system area (HSA) with licensed internal code.

- Establishing logically partitioned (LPAR) mode.
- Defining the input/output (I/O) configuration to the channel subsystem.

If you have experience using other systems, a power-on reset may have been referred to as an *initial microcode load* or *IML*.

On the Support Element workplace, the central processor complex (CPC) is the system, so the CPC is your target for a power-on reset.

Follow your local error recovery procedures for determining when to perform a power-on reset.

To perform a power-on reset:

1. You must have an input/output configuration data set (IOCDS) available on your Support Element which defines the I/O configuration for the CPC.
2. Locate the **CPC** to work with.

   Note: Performing a power-on reset to a CPC is considered disruptive. If the CPC is locked, unlock it. See **Object Locking for Disruptive Tasks**.
3. Open the **Power-on reset** task.

   The Power-On reset pages provide controls for customizing the information used to perform a power-on reset of the CPC.
4. Use the controls on each page to customize the power-on reset information as needed:
   a. Use the General page to select an operating mode and IOCDS for the CPC.
   b. Use the Dynamic page to establish the hardware support required to use dynamic input/output (I/O) configuration.
   c. Use the Options page to enable or disable the global input/output (I/O) priority queuing for the CPC and set the automatic input/output (I/O) interface reset.
5. Select **Perform power-on reset** to perform the power-on reset using the information you provided in the window.
6. Click **Power-on reset** to perform the power-on reset.

   The progress window indicates the progress of the power-on reset, and the outcome.
7. Click **OK** to close the window when the power-on reset completes successfully.

   If the power-on reset does not complete successfully, follow the directions on the window, or on any messages that may display, to determine the problem and how to correct it.

Power-on Reset

Use this task to manually perform a power-on reset of the central processor complex (CPC).

This lists all pages for the current profile.

- Profile tree pages

Additional functions on this window include:

Perform Power On Reset
To perform a Power On Reset, click **Power On Reset**.

Cancel
To close this window without continuing the hardware install, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Profile Tree

This lists all pages for the current profile.

- Profile tree pages

Pages

You can customize all the information necessary to perform a power-on reset of the central complex the CPC.

Make a selection from the Profile Tree to view the CPC pages:

General
To identify the Input/Output (I/O) configuration and operating mode to establish for the CPC activated by the profile, select **General**.

Storage
To customize the storage configuration to establish for the CPC upon performing the power-on reset, select **Storage**.

Dynamic
To customize information that controls whether the Input/Output (I/O) configuration established for the CPC upon performing the power-on reset can be dynamically changed, select **Dynamic**.

Options
To enable or disable global input/output (I/O) priority queuing and customize options for error handling and recovery for the CPC upon performing the power-on reset, select **Options**.

Fenced
Displays the number of available processors and processor assignments when a book is fenced.

General

Use this window to identify the Input/Output (I/O) configuration and operating mode to establish for the Central Processor Complex (CPC) upon performing the power-on reset.

IOCDS table

Select an Input/Output Configuration Data Set (IOCDS) to use during the power-on reset to define the Input/Output (I/O) configuration for the Central Processor Complex (CPC).

The I/O configuration is the set of all I/O devices and channel paths available to the CPC.

Input/Output Configuration Data Set
Displays the data set identifier and name of the IOCDS.

Type
Identifies the operating mode supported by the IOCDS. This must match the operating mode selected in

Note: A power-on reset cannot be performed if a mismatch exists between an IOCDS and mode.

Allow Dynamic I/O
Indicates whether the IOCDS defines an I/O configuration that supports dynamic changes.

Partitions
This column displays the names of logical partitions supported by the IOCDS.

Mode

Select the operating mode to establish during the power-on reset to support the number and type of control programs that can operate on the Central Processor Complex (CPC).

The mode determines some of the other types of information included in the reset profile. Different profile information is associated with each different mode. Only profile information associated with the selected mode will be saved.

Note: A power-on reset cannot be performed if a mismatch exists between an IOCDS and mode.

Storage

This window displays the storage available for allocating to the CPC's logical partitions upon performing power-on reset. The **Mode** list in **General** identifies the operating mode you selected for activating the CPC.

Displays the CPC's total amount of installed storage and storage available for allocating to the CPC's logical partitions.

Installed storage
Displays the CPC's amount of installed storage in megabytes.

Customer storage
Displays the storage amount available for allocating to the Central Processor Complex's (CPC) logical partitions.

Dynamic

Use this window to customize information that controls whether the Input/Output (I/O) configuration established for the Central Processor Complex (CPC) upon performing the power-on reset can be dynamically changed.

This window allows you to customize the Input/Output (I/O) configuration established for the Central Processor Complex (CPC) upon performing a power-on reset.

To set whether the I/O definition established for the CPC upon performing a power-on reset can be dynamically changed, select **Allow dynamic changes to the channel subsystem input/output (I/O) definition**.

If this is selected it indicates performing the power-on reset establishes an I/O definition that can be dynamically changed. That is, dynamic I/O will be enabled. Otherwise, this indicates the I/O definition cannot be changed dynamically. That is, dynamic I/O will not be enabled.

The input/output (I/O) definition is the set of all I/O devices and channel paths available to a central processor complex (CPC). An input/output configuration data set (IOCDS) is used during power-on reset as the source of the I/O definition.

Ordinarily, changing the I/O definition requires performing a power-on reset with a modified or different IOCDS. Dynamically changing the I/O definition does not require a power-on reset.

Dynamically changing the I/O definition requires support from the selected IOCDS and from the Hardware Configuration Definition (HCD) feature of a Multiple Virtual Storage (MVS) operating system.

Then the I/O definition can be changed dynamically by using the HCD feature of MVS.

Note: The active IOCDS must also support dynamically changing the channel subsystem I/O definition.

Options

Use this window to enable or disable the global input/output (I/O) priority queueing and customize options for error handling and recovery for the Central Processor Complex (CPC) upon performing the power-on reset.

Enable global input/output (I/O) priority queuing
To enable or disable global I/O priority queuing dynamically after initial microcode load (IML), select **Enable global input/output I/O priority queuing**.

Global I/O priority queuing allows the operating system to specify a priority to be associated with an I/O request at Start Subchannel time. These values are passed to the I/O subsystem for use when making queuing decisions with multiple requests.

Automatic input/output (I/O) interface reset
To indicate whether the I/O interface is reset automatically when any condition occurs that causes shared control units to hold reserves on their devices, select **Automatic input/output (I/O) interface reset**.

- A machine check places the Central Processor Complex (CPC) in a check stopped state.
- A control program places a logical partition in a non-restartable wait state.

If selected, the I/O interface is reset automatically if any of the listed conditions occurs. Otherwise, this indicates the I/O interface is not reset automatically.

In a multiple CPC environment, several objects, which can be CPCs or logical partition, may share the control units, channel paths, and I/O devices included in their I/O interfaces.

Each condition listed above causes shared control units to hold reserves on their devices for the object affected by the condition. Holding reserves provides the affected object with exclusive use of devices, preventing them from being used by other objects that share the control units.

Resetting the I/O interface releases reserves held by shared control units assigned to an object. Their devices become available to other objects.

Note: Automatically resetting the I/O interface will not recover the object from any of the conditions.

Set power saving
Use this window to select the energy management power saving option for the CPC upon performing the power-on reset. Power saving is used to reduce the average energy consumption of the system.

Custom energy management
To use the current power saving settings, select **Custom energy management**.

Emergency high performance
To use the high performance setting with no power saving, select **Emergency high performance**.

Fenced Book

This window displays the available system processors assigned when a hardware problem occurs with one of the system books that causes that book to be fenced or become unavailable for use.

- **Number of available processors for Licensed Internal Code** indicates the number of processors that are available in your system.
- **Number of available processors when a book is fenced** indicates the number of processors that your system can use when one book is fenced from use.
- **Number of available processors when a 17 processors book is fenced** indicates the number of processors that your system can use when a 17 processors book is fenced from use.
- **Number of available processors when a 20 processors book is fenced** indicates the number of processors that your system can use when a 20 processors book is fenced from use.

Processor assignment controls

Displays the processor assignment option.

Determined by the system
Select this option if you want the system to determine how to assign all available processors when a book is fenced from use in your system.

Determined by the user
Select this option if you want to manually assign the processors to your system when a book is fenced from use.

Processor assignments

Display processor assignment when a 17 processors book is fenced
Select this option to display the processor assignments when a 17 processors book is fenced.

Display processor assignment when a 20 processors book is fenced
Select this option to display the processor assignments when a 20 processors book is fenced.

Processor type
Displays the physical processor assigned to the logical partitions logical processors.

LICCC Definition
Displays the amount of licensed internal code installed in your system.

Value Used when Book is Fenced
Indicates how many processors have been assigned to the specified processor types.

Prepare System for Discontinuance

Prepare System for Discontinuance

This task prepares the system for end of service. Running this task permanently removes all Capacity on Demand records and system specific data.

PSW Restart

Accessing the PSW Restart task

A *restart* or *PSW restart* is a processor operation you can use to restart a processor. If you have experience using other systems, you may have used a RESTART command or Restart key to restart a processor.

Restarting a processor typically is done during a software error recovery procedure. Follow your local procedures for determining when to restart a processor. You can use the Support Element workplace to restart any eligible processor. Eligible processors include:

- Physical processors that support the image of a central processor complex (CPC).
- Logical processors that support the images of logical partitions activated in operating modes other than coupling facility mode.

To restart a processor:

1. Locate the **CPs** you want to work with.

   Note: Restarting a processor on an image can be considered disruptive. If the image is locked, unlock it.
2. Open the **PSW Restart** task.
3. Select a reason for restarting the processor, then click **OK** to continue.
4. Review the information on the PSW Restart Confirmation window to verify the processor that you will restart is the one you want.
5. If the information is correct, click **OK** to perform the restart.

   This begins the restart; a message displays when it is completed.
6. Click **OK** to close the message when the restart completes successfully.

   Otherwise, if the restart does not complete successfully, follow the directions in the message to determine the problem and how to correct it.

Query Coupling Facility Reactivations

Accessing the Query Coupling Facility Reactivations task

This task allows you to query what coupling facility current code level changes need to be deactivated and then reactivated in order to be applied to your CPC.

To query coupling facility reactivation:

1. Locate the **CPC** to work with.
2. Open the **Query Coupling Facility Reactivations** task.

   The Query Coupling Facility Reactivations window displays.
3. Review the list of coupling facility code level change to be reactivated.
4. Click **OK** to exit the window.

Query Internal Code Changes Pending Power on Reset

Accessing the Query Internal Code Changes Pending Power-On Reset task

Use this task to select a condition to either:

- View internal code changes currently pending a power-on reset.
- View summary of internal code changes pending power-on reset.

To query internal code changes pending power-on reset:

1. Locate the **CPC** to work with.
2. Open the **Query Internal Code changes Pending Power-On Reset** task.
3. Select the condition you want to view from the window.
4. Click **OK** to view the selected condition.

Query Internal Code Changes Pending Power-on Reset

Use this window to select a condition to either:

- View internal code changes currently pending a power-on reset
- View summary of internal code changes pending power-on reset.

View internal code changes currently pending a power-on reset
To display a list of internal code changes currently pending a power-on reset, select **View internal code changes currently pending a pending power-on reset.**

View summary of internal code changes pending power-on reset
To display a summary list of all internal code changes previously or currently pending a power-on reset, select **View summary of internal code changes pending power-on reset.**

OK
To perform the selected operation, click **OK**.

Cancel
To close the window and exit the task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Internal Code Changes Pending Power-On Reset Summary

Displays a summary list of all internal code changes previously pending a power-on reset or that are currently pending a power-on reset to activate or deactivate internal code changes. If the pending condition has already been cleared, then the status shows what action caused

Summary table
The summary table lists all internal code changes that have had a power-on reset previously or are currently pending a power-on reset for activation of internal code changes.

OK
To close the window and return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

Internal Code Changes Currently Pending Power-on Reset

Displays a list of the internal code changes that will be activated or deactivated on the next power-on reset. The changes have been installed or removed, but currently are not the active internal code levels on the system.

Pending level table
The pending table lists the current pending internal code changes that will be activated or deactivated on the next power-on reset.

OK
To close the window and return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

Reassign I/O Path

Accessing the Reassign I/O Path task

Reassign is an I/O operation you can use to perform, at once, all the steps necessary to reassign a reconfigurable I/O path from its owning logical partition to another logical partition:

Any I/O path that is reconfigurable is eligible for being reassigned. The reconfigurable I/O path displays **Reconfigurable**.

To reassign an I/O path:

1. The central processor complex (CPC) or physical channel identifier (PCHID) must be power-on reset.
2. The I/O paths must be defined as reconfigurable in the active I/O configuration.
3. Locate *one* reconfigurable I/O, identified with a physical channel identifier (PCHID), that you want to reassign.
4. Open the **Reassign I/O Path** task.

   The Reassign I/O Path window identifies the logical partition that the selected I/O path is currently assigned, and lists the logical partitions to which it can be reassigned.
5. Select from the list the logical partition that you want to reassign the I/O, then click **OK**.

   The Select a Partition window displays showing the ID and PCHID that is currently assigned, the owning partition, and a list of logical partitions from which you can select to reassign the I/O path.
6. Select the logical partition in the **Target Partition** window list to which you want the I/O path reassigned.
7. Click **OK**.

   The Confirm the Action window is displayed.
8. Click **OK** from the confirmation window to confirm your request to reassign the selected I/O path to the target logical partition.

   This reassigns the I/O path to the logical partition.

   Note: You may receive an additional warning that the I/O path will be released for reassignment if:

   - The partition isolation parameter is enabled.
   - The partition isolation parameter is disabled, but the logical partition to be reassigned was previously configured offline while the partition isolation parameter was enabled.

   Click **OK** to confirm the action.

Reassign I/O Path

Use this window to select the logical partition to which you want to reassign the selected input/output (I/O) path.

Note: You can reassign only one I/O path at a time.

The logical partition to which the I/O path is currently assigned is referred to as the *owning logical partition*. The logical partition to which you want to reassign the I/O path is referred to as the *target logical partition*.

Reassigning an I/O path includes:

1. Configuring off the I/O path from the owning logical partition, if the I/O path is currently configured on.
2. Releasing the I/O path from the owning logical partition, if the I/O path is currently isolated.

3. Configuring the I/O path on to the target logical partition, if activated.

   Note: If the target logical partition is not activated, the I/O path is still configured on, but its status does not immediately become **Online**. The status does not remain **Standby**. It will be Online Pending and will go to **Online** when the logical partition is activated.

Identifier (ID) table
This table lists the I/O paths that can be reassigned including the following information:

ID
This can display a two-digit number followed by a decimal followed by a two-digit number. The number before the decimal is the Channel Subsystem (CSS) number and the number after the decimal is the CHPID number of the I/O path that will be reassigned.

This can also display a four-digit number that represents a function identifier (FID) for the channel.

PCHID
Displays a four-digit physical channel identifier (PCHID) of the channel.

Owner
Displays the name of the logical partition to which the channel path is currently assigned.

State
Displays **Online** when the target logical partition is activated, displays **Online Pending** until the target logical partition is activated, or displays **Standby** if the target logical partition is not activated.

Type
Specifies the name of the device.

OK
To reassign the selected I/O path to another logical partition, click **OK**.

Refresh
To discard the selections you made to the Reassign I/O Path window and display again the selections that displayed when you opened this task, click **Refresh**.

Cancel
To close this window without reassigning the I/O path, click **Cancel**.

Help
To display help for the current window, click **Help**.

Select a Partition

Use this window to select a partition to which the I/O path should be reassigned.

Identifier (ID)
Displays a two-digit number followed by a decimal followed by a two-digit number. The number before the decimal is the Channel Subsystem (CSS) number. The number after the decimal is the CHPID number of the I/O path that will be reassigned. It can also display a four-digit number that is the function identifier (FID).

Physical channel identifier (PCHID)
Displays a four-digit physical channel identifier (PCHID) of the channel.

Owning partition
Displays the name of the logical partition to which the I/O path is currently assigned.

Target partition
Displays the name of the logical partition to which the I/O path will be reassigned.

OK
To reassign the selected I/O path to another logical partition, click **OK**.

Cancel
To close this window without reassigning the I/O path, click **Cancel**.

Help
To display help for the current window, click **Help**.

Confirm the Action

Use this window to confirm or cancel your request to reassign the selected I/O path from the owning logical partition to the target logical partition.

Review the information in the fields, then make a selection.

Identifier
Displays a two-digit number followed by a decimal followed by a two-digit number. The number before the decimal is the Channel Subsystem (CSS) number. The number after the decimal is the CHPID number of the I/O path that will be reassigned. It can also display a four-digit number that is the function identifier (FID).

Physical channel identifier (PCHID)
Displays a four-digit physical channel identifier (PCHID) of the channel that will be reassigned.

Owning partition
Displays the name of the logical partition to which the I/O path is currently assigned.

Target partition
Displays the name of the logical partition to which the I/O path will be reassigned.

OK
To confirm your request to reassign the I/O path from the owning logical partition to the target logical partition, click **OK**.

Cancel
To cancel your request and close this window without reassigning the I/O path, click **Cancel**.

Help
To display help for the current window, click **Help**.

Rebuild Vital Product Data

Accessing the Rebuild Vital Product Data task

Note: Do not rebuild the Vital Product Data unless you have been directed by product support.

This task forces a rebuild of the Vital Product Data on the Support Element. Before a rebuild is done, the current version will be saved.

To rebuild the vital product data:

1. Locate the system to work with.
2. Open the **Rebuild Vital Product Data** task. The Rebuild Vital Product Data window is displayed.
3. **Click OK** to continue with this task.
4. After the vital product data is rebuilt, a message displays that the rebuild was successful.
5. Click **OK** to complete the task.

   Note: If a failure occurs, an error will be logged in the default system log.

Rebuild Vital Product Data

Do not rebuild the Vital Product Data (VPD) unless you have been directed by product support to do so.

The VPD for a Support Element contains the following data:

- The location, part number, and serial number of the system
- The locations, part numbers, and serial numbers of the installed parts and features
- Installed Engineering Changes (ECs)
- The level of licensed internal code.

If the rebuild of the VPD fails, the backup VPD data file (iqyvpd2b.dat) is not restored.

OK
To continue with your request to rebuild Vital Product Data, click **OK**.

Cancel
To cancel your request to rebuild Vital Product Data, click **Cancel**.

Help
To display help for the current window, click **Help**.

Redundant I/O Interconnect Status and Control

Accessing the Redundant I/O (RIO) Interconnect Status and Control task

This task allows you to check the state and status of the Redundant I/O (RIO) multiport and chain links for the InfiniBand and PCIe channel types. An option is also available to display details and search a specific PCHID/CSS.CHPID controlled by the selected channel.

To check RIO multiport status:

1. Locate the **CPC** to work with.
2. Open the **Redundant I/O Interconnect Status and Control** task.

   The Redundant I/O Interconnect Status and Control window displays.
3. Click **Display PCHID/CSS.CHPID** to display details for both sides of the RIO multiport.
4. Click **Search PCHID/CSS.CHPID** to search for a specific PCHID/CSS.CHPID.
5. Click **Cancel** to close the window.

Redundant I/O Interconnect Status and Control

Use this window to display the state and status of the Redundant I/O Interconnect (RIO) multiport and chain links. You can display details of a selected RIO multiport and associated PCHID/CSS.CHPID(s) controlled by that RIO multiport. A search option is available to locate a RIO multiport associated with specific PCHID/CSS.CHPID.

Redundant I/O Interconnect Status and Control table
The table displays information on specific RIO multiport and associated PCHID/CSS.CHPID.

Attention
Displays "> > >" when a status of something on the multiport link is not normal.

PBU Link 1 to Fanout Status-Speed-Width
Displays the PBU Link 1 fanout status-speed-width.

Fanout Link 1 to IO Status-Speed-Width
Displays the fanout Link 1 location to IO status-speed-width.

Multiport Link 1 Cage-Slot-Jack
Displays the location of the cage, slot, and jack location of the multiport link 1.

Multiport Link 1 I/O Cage-Slot
Displays the location of the cage, slot, and jack location of the multiport link 1.

Chain Link Status-Speed-Width
Displays the state of the chain link between the Multiport Link 1 and 2. The status can be Operational, Standby, or Unknown.

Multiport Link 2 I/O Cage-Slot
Displays the I/O cage and slot location of the multiport link 2.

Multiport Link 2 Cage-Slot-Jack
Displays the location of the cage, slot, and jack location of the multiport link 2.

Fanout Link 2 to IO Status-Speed-Width
Displays the fanout Link 1 location to IO status-speed-width.

PBU Link 2 to Fanout Status-Speed-Width
Displays the PBU Link 2 fanout status-speed-width.

Display PCHID/CSS.CHPID
To display the PCHID/CSS.CHPID Details for both sides of the RIO multiport on the selected RIO multiport row, click **Display PCHID/CSS.CHPID**.

Search PCHID/CSS.CHPID
To search for a specific PCHID/CSS.CHPID, click **Search PCHID/CSS.CHPID**.

Cancel
To return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Redundant I/O Multiport PCHID/CSS.CHPID Details

Use this window to display Redundant I/O Multiport PCHID/CSS.CHPID Details for the selected RIO multiports. If the PCHID is not defined in the IOCDS, the CSS.CHPID fields are blank.

RIO multiport side 1
Displays the cage-slot location and possible associated PCHID/CSS.CHPID(s) for RIO multiport side 1.

RIO multiport side 2
Displays the cage-slot location and possible associated PCHID/CSS.CHPID(s) for RIO multiport side 2.

OK
To perform the selected operation, click **OK**.

Search for PCHID or CSS.CHPID

Use this window to enter a PCHID/CSS.CHPID and display the RIO multiport row that controls that PCHID/CSS.CHPID.

Enter the PCHID or the CSS.CHPID to search for
Enter the PCHID or the CSS.CHPID you want to search for.

OK
To perform the search operation, click **OK**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Release I/O Path

Accessing the Release I/O Path task

Release is a CHPID operation you can use to free reconfigurable I/O paths from their assignment to isolated logical partitions.

The active input/output configuration data set (IOCDS) determines whether channel paths are reconfigurable, and which logical partition each I/O path is assigned to. Each logical partition's security settings determine whether it is isolated. A logical partition's initial security settings are set by the activation profile used to activate it. Afterwards, the **Change LPAR Security** task can be used to change the settings. For more information, see the **Change LPAR Security** task.

Reconfigurable I/O paths assigned to an isolated logical partition do not become available to other logical partitions when they are configured off. Releasing such I/O paths will make them available to other logical partitions.

I/O paths that are both reconfigurable and isolated are eligible for being released. The reconfigurable I/O path displays **Shared** or **Dedicated** and either **Isolated** or **Not isolated** to indicate whether it is assigned to an isolated logical partition.

To release I/O paths:

1. The central processor complex (CPC) must be power-on reset.
2. The I/O paths must be defined as reconfigurable in the active input/output (I/O) configuration.
3. The I/O paths must be assigned to isolated logical partitions.
4. The I/O paths must be configured off.
5. Locate the reconfigurable I/O paths you want to release.
6. Open the **Release I/O Path** task.
7. Click **OK** from the confirmation window to confirm your request to release the selected I/O paths.

   This releases the I/O paths.

Note: Upon configuring off and releasing reconfigurable I/O paths from isolated logical partitions, you must use operating system facilities to configure them on to other logical partitions.

Release I/O Path Confirmation

Use the Release I/O Path Confirmation window to confirm or cancel your request to release the selected reconfigurable I/O paths from the logical partitions to which they are currently assigned.

Releasing isolated reconfigurable I/O paths from the logical partitions to which they are currently assigned makes them available for being configured on to other logical partitions.

Note: Although you can also release reconfigurable I/O paths that are not isolated, it is not necessary, since they are already available for being configured on to other logical partitions.

Isolated
Reconfigurable I/O paths are referred to as *isolated* if they are assigned to a logical partition that is activated with logical partition isolation enabled.

Logical partition isolation is a setting in a logical partition's image profile that controls whether its reconfigurable I/O paths become available to other logical partitions when the I/O paths are configured off:

- When a logical partition is activated with logical partition isolation disabled, its reconfigurable I/O paths become available to other logical partitions when the I/O paths are configured off.
- When a logical partition is activated with logical partition isolation enabled, its reconfigurable I/O paths are isolated, and do not become available to other logical partitions when the I/O paths are configured off.

  Instead, after an isolated I/O path is configured off, it must also be *released* to make it available to other logical partitions.

Channel path identifier list
Displays a list of channel path identifiers (IDs) of the reconfigurable I/O paths you selected to release.

OK
To confirm your request to release the selected reconfigurable I/O paths from the logical partitions to which they are currently assigned, click **OK**.

Cancel
To cancel your request and close this window without releasing any I/O paths, click **Cancel**.

Help
To display help for the current window, click **Help**.

Remote Service

Accessing the Remote Service task

Remote service is a two-way communication between the console and the support system for conducting automated service operations.

You can use the Support Element workplace to customize the remote service settings of the system. The settings control whether and how the system's Support Element uses the remote support to establish a remote connection through its call-home server to your service provider's service support system. Whenever a connection is established during a Support Element operation, it can send information to the support system or receive information from it.

To customize remote service settings:

1. Locate the system to work with.
2. Open the **Remote Service** task.
3. Use the Customize Remote Service window to set the system's remote service settings.
4. Select **Enable remote service request**. This option allows the Support Element to establish remote connections to the support system.
5. To allow the Support Element to automatically report problems and get service through its remote connection to the support system:
   - Select **Authorize automatic service call reporting** to enable service for related problems.
   - Select **Authorize service personnel to remotely request transmission of service data** to allow the system to process service data requests downloaded from the support system.
6. You must customize the telephone number the console's hardware messages will include as an option for reporting problems.
7. Click **OK** to save the settings and close the window.

Connecting and communicating with a remote service support system

Remote service is two-way communication between the Support Element of a system and a remote, automated *service support system* provided and maintained by the system's service provider. For example, when IBM is the system's service provider, IBM provides and maintains the remote, automated support system.

The system’s *remote service settings* control whether and how its Support Element uses remote service. When the system's remote service settings are customized for using remote service, the system's Support Element uses remote support to establish a remote connection through its *call-home server* to your service provider's service support system. Whenever a connection is established during a Support Element operation, it can send information to the service support system or receive information from it.

Using remote service is optional, but has the following benefits:

- You can let the Support Element automatically report problems and get service through the support system.
- You can use the support system as a source for retrieving internal code changes.
- You can use the support system as a destination for transmitting service data.

The remaining topics in this section describe these benefits in more detail and provide instructions for getting them by customizing the system’s remote service settings.

Getting ready to report problems and get service

The Support Element automatically and continuously monitors itself and the system for problems. If the Support Element detects a problem, it uses a knowledge-based expert system called *Problem Analysis* to automatically:

- Analyze the problem, attempt to determine its cause, and determine whether service is required to correct the problem.
- Issue a hardware message to notify you of the problem. Information provided with the message includes a detailed description of the problem and instructions for correcting it or calling for service.
- Send problem information for optical errors to a designated console, if available, for additional analysis.

If service is required to correct the problem, it is your responsibility to contact your service provider, report the problem, and request service to correct it. You can do this manually by calling your service provider on the telephone and using the information provided with the hardware message to describe the problem.

If your service provider has an automated support system for receiving and processing problem reports and service requests, you can report problems and request service automatically by customizing the Support Element's remote service settings as follows:

- *Enable* remote service to allow the Support Element to establish remote connections through its *call-home server* to your service provider's support system.
- *Enable* automatic service calling to allow the Support Element to automatically report problems and get service through the remote connection to the support system.

If the Support Element detects a problem while remote service and automatic service calling are enabled, the Support Element uses its call-home server to transmit the problem report and service request to the support system, which receives and processes them according to the service policies of your service provider. For example, the support system analyzes your problem report, then forwards it accordingly:

- When the cause of the problem is known, the support system forwards the problem report to a service representative, who is then sent to your location with the instructions, parts list, and other information necessary to correct the problem.
- When the cause of the problem is not yet known, the support system forwards the problem report for further analysis.

Getting ready to retrieve internal code changes

Licensed internal code, referred to also as *internal code*, controls many of the operations available on a system and its Support Element. *Internal code changes* are provided to change the internal code of a system or its Support Element. Changing the internal code may be necessary to add new functions, improve existing functions, or correct problems.

Internal code changes are delivered on a USB flash drive and by making them available on the support system. Although the same internal code changes are available from each source, the most direct source is the support system. But you can use the support system as a source only by customizing, in advance, the system's remote service settings to *enable* remote service.

While remote service is enabled, the support system is *another* source for manually retrieving internal code changes. If you intend to *schedule an operation* for retrieving internal code changes regularly and automatically, the support system is the only eligible source. You must enable remote service before scheduling an operation for retrieving internal code changes.

Getting ready to transmit service data

Service data is a set of system information, such as program and event traces and storage dumps, collected by the Support Element of the system. When IBM is the service provider for your system, service data assists IBM in servicing it.

You can send service data either by copying it to a removable media for delivery, or by transmitting it through a remote connection to the support system. Although the same service data is sent through each destination, the most direct destination is the support system. You can use the support system as a destination only by customizing, in advance, the system's remote service settings to *enable* remote service.

While remote service is enabled, the support system is *another* destination for manually transmitting service data. If you intend to *schedule an operation* for transmitting service data regularly and automatically, the support system is the only eligible destination. You must enable remote service before scheduling an operation for transmitting service data.

Remote Service

Use this window to customize the console for using remote service.

Remote service is two-way communication between the console and the support system for the purpose of conducting automated service operations. Using remote service reduces the operator interaction needed to complete some service operations and provides some console tasks with another source or destination for sending or receiving service information.

The controls you will use to customize the console's remote service settings are determined by whether you want to enable or disable remote service.

Controls for enabling remote service

Enable remote service if you want to allow console connections to the support system.

Select Enable remote service requests to enable remote service. If it is not selected remote service is disabled.

After enabling remote service, customize how service calls are reported:

Authorize automatic service call reporting
To set the console to automatically report problems and request service, select **Authorize automatic service call reporting**.

"Authorize service personnel to remotely request transmission of service data" on page 790
To set the console to allow service support to remotely request the transmission of service data, select **Authorize service personnel to remotely request transmission of service data**.

Customer Service Center Telephone Number
This field displays the telephone number the console's hardware messages will include as an option for reporting problems and requesting service if automatic service call reporting is disabled. You can change the telephone number whenever necessary.

Additional functions are available from this window:

OK
To continue with the remote service configuration you have selected, click **OK**.

Cancel
To exit this window without configuring for remote service, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Enable remote service requests

To enable remote service, select **Enable remote service requests**.

About remote service

Remote service is two-way communication between the console and the support system for the purpose of conducting automated service operations.

- *Enable* remote service if you want to allow console connections to the support system (a check mark appears).
- *Disable* remote service if you do *not* want to allow console connections to the support system (a check mark does not appear).

Using remote service reduces the operator interaction needed to complete some service operations and provides some console tasks with another source or destination for sending or receiving service information. For example, by using remote service:

- You can allow the console to automatically report problems and request service through the support system.
- You can use the support system as a source for retrieving internal code changes.
- You can use the support system as a destination for transmitting service data.

Authorize automatic service call reporting

If remote service is enabled, select **Authorize automatic service call reporting** to set the console for authorization to automatically report problems that require service (referred to as *automatic service call reporting*).

About automatic service call reporting

The console issues hardware messages to notify console operators of problems that require service. When automatic service call reporting is authorized, the console can automatically report problems and request service through console connections to the support system.

Otherwise, when automatic service call reporting is *not* authorized, a console operator must decide how to report problems and request service. A problem's hardware message provides two options:

- Calling the customer service center to speak to a service representative.
- Or manually authorizing the console to make the service call through a console connection to the support system.

Authorize service personnel to remotely request transmission of service data

If remote service is enabled, select **Authorize service personnel to remotely request transmission of service data**. This option allows the system to process service data requests downloaded from the support system.

Customer Service Center Telephone Number

Displays the telephone number of the customer service center console operators can call to speak to a service representative about product problems and service.

If remote service is disabled, the console includes the customer service center telephone number in the hardware messages it issues to notify console operators of problems that require service. Such hardware messages typically instruct the console operator to call the customer service center to report the problem and request service.

But the customer service center telephone number is required *even when remote service is enabled*. The console may not always be able to automatically report a problem that requires service, and will issue a hardware message to instruct the console operator to call the customer service center instead. For example:

- The console may fail to connect to the support system while making a service call.
- The console may not be authorized to automatically make service calls.

  Note: In this case, hardware messages for problems that require service provide two options: calling the customer service center or manually authorizing the console to make the service call.

Removable Media or FTP Server

Removable Media or FTP Server

Use the removable media or FTP server window to copy data from the selected media.

/console/data
To copy console data, select **/console/data**.

USB media
To copy data from a USB flash memory drive, select **USB media**.

Then insert a USB flash memory drive into a USB port, and click **OK**.

Note: If you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed.

Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

FTP server
To copy data from an FTP server, select **FTP server**. Use the **Protocol** field to specify a secure network protocol for transferring files to the specified FTP destination. Use the **File path** field to type the file path directory where the files are to be saved or read.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the Manage SSH Keys task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

OK
To copy data from the selected media device or FTP server, click **OK**.

Cancel
To close this window without copying data from the selected media or FTP server, click **Cancel**.

Help
To display help for the current window, click **Help**.

Report a Problem

Accessing the Report a Problem task

Problem Analysis provides the means for reporting a problem and requesting service only if it identifies the problem and determines service is required to correct the problem. While Problem Analysis provides very comprehensive problem identification and determination, if it does not identify or does not determine service is required for a problem you suspect is affecting the system or Support Element, you can use the Support Element workplace to report the problem and request service anyway, independently of the results of Problem Analysis.

To report a problem and request service independently of Problem Analysis:

1. Locate the systems to work with.
2. Open the **Report a Problem** task.
3. Select the type of the problem you have from the list provided and enter a description of the problem in the **Problem Description** box.

Note: If you are just testing problem reporting, select **Test automatic problem reporting** and enter *This is just a test* in the **Problem Description** box.

4. Click **Request Service**.

To test problem reporting from the Report a Problem window:

1. Select **Test automatic problem reporting** and enter This is just a test in the Problem Description input field.
2. Click **Request Service**. The Report Problem window is displayed.
3. Click **OK** to complete this task.

Report a Problem

Use this window to either:

- Report a problem that occurred on the selected system, and to request service to repair it.
- Or test whether problems can be reported for the system (if testing is supported by the system's Support Element).

Problems are reported to the service provider for the selected system. Reporting a problem sends to the service provider the information you provide on this window, and machine information that identifies the system.

Ordinarily, Problem Analysis automatically detects error conditions, and reports to you any problem that requires service to repair it.

However, if you notice a problem occurred or you suspect a problem is affecting the system, but Problem Analysis has not reported it to you, then use this window to report the problem to the service provider.

Problem Type

Use this section of the window to either:

- Select the problem type that best describes where the problem occurred or what the problem affected on the selected system.
- Or test whether problems can be reported for the system (if testing is supported by the system's Support Element).

Possible problem types include:

Power
To report a problem with the power subsystem of the selected system, select **Power**.

CPC
To report a problem with hardware in the processor subsystem of the selected system, select **CPC**.

LAN
To report a problem with the local area network (LAN) that attaches the selected system, select **LAN**.

Software
To report a problem with an operating system or other software loaded on the selected system, select **Software**.

I/O
To report a problem with hardware in the input/output (I/O) configuration of the selected system, select **I/O**.

Health Check
To report the state of the system before applying a maintenance action (such as: driver upgrades, MCLs, MES adds), select **Health Check**.

Other
To report a problem with the selected system that is not adequately described by any other problem type, select **Other**.

Test automatic problem reporting
To test whether problems can be reported for the selected system, select **Test automatic problem reporting**.

Note: This option is displayed only if testing problem reporting is supported by the Support Element of the selected system.

Problem Description

Specify an explanation of the problem that occurred on the selected system.

Your comments will assist the service provider for the system with correctly determining the cause of the problem.

Additional functions are available from this window:

Request Service
To report the problem and request service to repair it, click **Request Service**.

Problems are reported to the service provider for the selected system. Reporting a problem sends to the support system the information you provide on this window, and machine information that identifies the system.

If this console is customized to use the Remote Support Facility (RSF) and is authorized to automatically call for service, the problem information and service request are sent to the support system automatically.

Otherwise, additional windows will be displayed to request you authorize an automatic service call, or to provide you with the instructions and information you need to manually contact the support system, request service, and describe the problem.

After the support system receives the service request, a service representative can be sent to the repair site, and can be prepared to repair the problem upon arriving.

Cancel
To exit this task without reporting a problem, click **Cancel**.

Help
To display help for the current window, click **Help**.

Test automatic problem reporting

To test whether problems can be reported for the selected system, select **Test automatic problem reporting**.

To report problems for the system:

- Remote service must be enabled for the system.
- The system must have at least one call-home server.

If the system is configured correctly for reporting problems, testing it will open a Type 1 problem. You should specify a description in the **Problem description** field to indicate it is only a test. Then click **Request Service** to start the test.

Notes:

- This option is displayed only if testing problem reporting is supported by the Support Element of the selected system.
- Problem reporting typically is tested during system installation.
- Use the **Remote Service** task to enable remote service and customize remote service settings for the system.
- The system's call-home servers can include this Hardware Management Console, other Hardware Management Consoles, and the systems's Support Element console if it is stand-alone Support Element. To configure **this** console as a call-home server for the system:

1. Use the **Change Object Definition** task to identify the console as a call-home server for the system.
2. Use the **Customize Outbound Connectivity** task to enable and access the console's call-home server service.

Reset Clear

Accessing the Reset Clear task

To perform a reset clear:

1. Locate the **Image** you want to work with.

   Note: Performing a reset clear on an image can be considered disruptive. If the image is locked, unlock it.
2. Open the **Reset Clear** task.
3. Review the information on the confirmation window to verify the image you will reset.
4. If the information is correct, Click **Yes** to perform the reset clear.

   The progress window indicates the progress of the reset, and the outcome.
5. Click **OK** to close the window when the reset completes successfully.

   If the reset does not complete successfully, follow the directions on the window, or on any messages that may display, to determine the problem and how to correct it.

Reset Error Thresholds

Reset Error Thresholds

This window displays a list of selected PCHIDs that you want to reset the threshold that was used to stop reporting Interface Control Checks (IFCCs) and Bit Errors (BERs).

PCHID table
Lists the PCHIDs that require a reset error threshold.

OK
To reset the error threshold for the list of PCHIDs, click **OK**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Reset Normal

Accessing the Reset Normal task

A *reset normal* initializes a system or logical partition by:

- Clearing its pending interruptions.
- Resetting its channel subsystem.
- Resetting its processors.

If you have experience using other systems, a reset normal may have been referred to as a *system-reset-normal*.

A reset normal prepares a system or logical partition for loading it with an operating system. On the Support Element workplace, *images* support operating systems, images are your targets for resets. An image represents a logical partition, while the CPC is activated.

A reset normal is one of several recovery tasks that you can use to attempt to recover from hardware or software errors. A reset normal is often effective but less disruptive than other tasks, which typically

makes it the first task attempted to recover from errors when they occur. Follow your local error recovery procedures for determining when to perform a reset normal.

To perform a reset normal:

1. Locate the **Image** you want to work with.

   Note: Performing a reset normal on an image can be considered disruptive. If the image is locked, unlock it.
2. Open the **Reset Normal** task.
3. Review the information on the confirmation window to verify the image you will reset.
4. If the information is correct, Click **Perform reset** to perform the reset normal.
5. Click **OK** to close the progress window when the reset completes successfully.

   Otherwise, if the reset does not complete successfully, follow the directions on the window, or on any messages that may display, to determine the problem and how to correct it.

Reset Swap Channel Path

Reset Swap Channel Path

Reset swap channel path restores the original association between the physical channel identifiers (PCHIDs) and physical channels of two swapped channel paths.

The action applies to the two PCHIDs that display the **Swapped** status. When the operation completes, the original channel path status displays.

Channel path swapping is used for channel problem isolation. A channel path swap usually is performed with a corresponding physical swap of channel cables. The operation provides a means of redirecting I/O operations from one swapped channel path to the other, without actually changing the I/O configuration defined to the operating system.

Note: If the channel cables were physically swapped when the channel path swap was performed, the cables must be restored to their original positions when a reset is performed.

Note: Refer to "Channel Swap Procedure" in the *zEnterprise EC12 Service Guide*, GC28-6915.

OK
To reset the channel paths of the selected swapped channels, click **OK**.

Cancel
To cancel the reset of the selected swapped channels, click **Cancel**.

Help
To display help for the current window, click **Help**.

Save Upgrade Data

Accessing the Save Upgrade Data task

This task saves all of the upgrade data for your console to the hard drive or USB flash memory drive before performing an Engineering Change (EC) upgrade.

To save the console upgrade data to the hard drive:

1. Open the **Save Upgrade Data** task. The Save Upgrade Data window is displayed.
2. Select **Hard drive**. It takes from one to five minutes to save the data.
3. When the data is saved, the Save Upgrade Data Completed window is displayed.
4. Click **OK** to end the task.

Save Upgrade Data

Use this window only while following an Engineering Change (EC) upgrade procedure that instructs you to save the console's upgrade data.

The console's *upgrade data* is information on its hard disk that is unique to it. Upgrading the console requires saving its upgrade data *before* installing new ECs, then restoring the upgrade data afterwards.

Some EC upgrade procedures save and restore the console's upgrade data automatically, and there is no need to use this task. Otherwise, if you are following an EC upgrade procedure that instructs you to save the console's upgrade data, you must use this task to save it manually.

Hard drive
To save the console's upgrade data to the hard drive, select **Save to hard drive**.

USB flash memory drive
To save the console's upgrade data to the USB flash memory drive, select **Save to USB flash memory drive**.

The USB flash memory drive for the Save Upgrade Data task must be formatted with a value label of **ACTUPG**, using the **Format Media** task.

Note: When you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

OK

To save the upgrade data to the selected location, click **OK**.

When you select **USB flash memory drive**, the **Select Media Device** window is displayed. From this window you can choose the media you want to send the data to. You can click **OK** to continue with the task, click **Refresh** to redisplay your media selections, or click **Cancel** to return to the previous window.

Refresh
To redisplay the list of available media, click **Refresh**. Use this option if you did not insert your media before this point in the task.

Cancel
To cancel this task, click **Cancel**.

Help
To display help for the current window, click **Help**.

Save/Restore Customizable Console Data

Accessing the Save/Restore Customizable Console Data task

This task, used by an access administrator or a user ID that is assigned access administrator roles, enables you to save the following customizable Support Element data:

User Profile Data
User identifications, authentication mode and roles, password rules, user pattern definitions, user template definitions, user settings that were created and retained, in addition to LDAP servers and optional LDAP user IDs.

Group Data
All user-defined group definitions.

SNMP API Settings
SNMP API configuration information.

To save or restore customizable console data:

1. Open the **Save/Restore Customizable Console Data** task. The Save/Restore Customizable Console Data window is displayed.
2. Select one or more data types you want to save or restore.
3. Use the default file name to save the data to or restore the data from or specify your own in the **File name** input field.
4. Click **Save** to save data to USB flash memory drive or FTP sever, or click **Restore** to restore data from USB flash memory drive or FTP server.
5. Proceed with the your selection of USB flash memory drive or FTP server, or click **Cancel** to go back to the previous window without saving or restoring the data.

Save/Restore Customizable Console Data

Use this window to distribute the same customizable console data among multiple consoles.

Customizable console data is data that is customized by users to set up how the console works. By saving and restoring customizable console data, you can easily tailor multiple consoles to have, for example, the same user IDs, user groups, domain, and look and feel.

Use this window first to save the customized data for a console that is customized the way that you want it. Then, restore that console's customizable data at each other console you want to work the same way.

You can save or restore one or more of the following types of customizable console data for a console:

- User Profile Data
- Group Data
- SNMP API Settings

Customizable Data Types

Use this window to save or restore customizable data for the console.

You can work with the list of customizable data types by using the table icons or the **Select Action** drop-down list from the table tool bar. If you place your cursor over an icon, the icon description is displayed. The icons perform the following functions in the Customizable Data Types table:

Select All
Selects all data types in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Deselect All
Deselects all data types in the table. You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for the columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header to change from ascending to descending order. Click **OK** when you have defined your preferred order.

Clear all sorts
Returns the table back to the default order.

The types of customizable data that can be saved or restored are:

User Profile Data
User identifications, authentication mode and roles, password rules, user pattern and user template definitions, user settings that were created and retained for template user identifications, in addition to LDAP servers and optional LDAP user IDs.

Group Data
All user-defined group definitions.

SNMP API Settings
SNMP API configuration information.

By saving and then restoring one or more of these types of data, multiple consoles can easily be tailored to work and look the same.

USB flash memory drive

To save the console's customizable data to the USB flash memory drive, select **USB flash memory drive**. The USB flash memory drive for this task must be formatted with a value label of **ACTUPG**, using the **Format Media** task.

Note: When you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

FTP server

To save the console's customizable data to an FTP server, select **FTP server**.

File name

Use this entry field to specify the file name to use for saving or restoring customizable console data. You can save it to or restore it from a USB flash memory drive.

Note: When you use a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message is displayed indicating the drive was not added and that you should remove the device and try again.

The file name will be a fully-qualified file name. The default name is **ccdata.dat**, which appears in the input field, and is appended to a fully qualified name once you have selected your media device.

You can also specify your own file name. For example, you can specify **myfile.dat** in the input field. If you selected a USB flash memory drive as your media device, then the fully qualified name is **/media/xxxx/myfile.data**, where **xxxx** is the unique ID of the USB in use.

Additional functions are available from this window:

Save
To save the specified customizable console data, click **Save**.

When a file name is specified, the **Select Media Device** message window is displayed. From the **Select Media Device** message window, select the type of media you want to save the data to. Then, either, click **OK** to save the data, click **Refresh** to refresh the list of available media, or click **Cancel** to go back to the previous window before saving to media.

Restore
To restore the specified customizable console data, click **Restore**.

When a file name is specified, the **Select Media Device** message window is displayed. From the **Select Media Device** message window, select the type of media you want to restore the data from. Then, either, click **OK** to restore the data, click **Refresh** to refresh the list of available media, or click **Cancel** to go back to the previous window before restoring from media.

Cancel
To end this task without saving or restoring data, click **Cancel**.

Help
To display help for the current window, click **Help**.

Select Media Device

Use this window to select the device to which the files will be saved to or restored from.

OK
To continue the task with the selected media, click **OK**.

Refresh
To update the device list, click **Refresh**.

Cancel
To exit this window without making any changes and to return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

File Transfer Information

Use this window to configure FTP settings when you use an external server to save or restore your files.

Host name
Specify the host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

OK
To apply this information, click **OK**.

Clear
To remove all information from the input fields, click **Clear**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Selective Channel Patch Controls

Accessing the Selective Channel Patch Control task

Use this task to selectively define which OSA-Express channels will have new channel loads applied via a concurrent code update.

To select channel apply updates:

1. Locate the **CPC** to work with.
2. Open the **Selective Channel Patch Control** task

   The Selective Channel Patch Control window displays.
3. Select the channel type you want to apply updates.

   Note: The selected channel type will require a configure off/on of each channel for the selected channel type.
4. Click **OK** to perform the operation.
5. Click **Cancel** to exit the window without performing the operation.

Selective Channel Patch Controls

Use this window to selectively define which OSA-Express type channels and/or cryptos will have new channel loads applied with a concurrent code update.

When a channel type and/or crypto is selected, a configure off/on of each channel for the selected channel type and/or crypto is required.

Microcode Component Types

The selective patch control is available for the following channel types:

- OSA-Express5S / OSD for QDIO
- OSA-Express5S / OSM
- 3270 OSA-Express5S
- 3215 OSA-Express5S
- OSA-Express6S / OSD for QDIO
- OSA-Express6S / OSM
- 3270 OSA-Express6S
- 3215 OSA-Express6S
- OSA-Express7S / OSD for QDIO
- OSA-Express7S / OSM
- 3270 OSA-Express7S
- 3215 OSA-Express7S
- Crypto Express5S CCA Coprocessor or Accelerator
- Crypto Express6S CCA Coprocessor or Accelerator
- Crypto Express6S EP11 Coprocessor or Accelerator
- Crypto Express7S CCA Coprocessor or Accelerator
- Crypto Express7S EP11 Coprocessor or Accelerator

Each channel for the specified channel type will require a configure off/on in order to perform a code load.

OK

To close the window and return to the previous window, click **OK**

Cancel

To close the window without saving changes you made, click **Close**.

Help
To display help for the current window, click **Help**.

Service On/Off

Accessing the Service On/Off task

Service on and *Service off* are channel operations you can use to control whether channels, identified with physical channel identifiers (PCHIDs) are on standby in, or reserved from, the active input/output (I/O) configuration:

- A channel is on *standby* while service is set off. It is in the active I/O configuration but it cannot be used until it is configured on. It will remain in the active I/O configuration until service is set on.
- A channel is *reserved* while service is on. It is not in the active I/O configuration and cannot be used. It will remain out of the active I/O configuration until service is set off.

Setting service on for a channel, which removes it from the active I/O configuration, allows running diagnostic tests on the channel without disturbing other channels being used by the system. Setting service on for a channel can be used also to remove failing channels from the I/O configuration so subsequent power-on resets will not attempt to initialize the failing channels.

If you have experience using other systems, setting service on or off for channels may have been referred to as taking channels in and out of single channel service (SCS), for which you may have used an SCS command with IN and OUT parameters.

To set service on and off for a channel:

1. Open the **Service On/Off** task.
2. Initially, each channel's current state and target state are the same. Use the Service On/Off window controls to change the target states of the channel that you want to set the service state on or off:
   - If the current state of a channel is **Reserved**, toggle its target state to **Standby** if you want to set service off for the channel.
   - If the current state of a channel is **Standby**, toggle its target state to **Reserved** if you want to set service on for the channel.

   If you attempt to change the target state of a channel that cannot have service set on or off, a message is displayed in the **Messages** list column to indicate changing the channel's state is not allowed. Double-click on the message for more information about why the channel state cannot be changed.
3. When you finish changing the target states of the channels for which you want to set service on or off, click **Apply** to make each channel's new target state its current state.
4. When you finish changing the target states of the object you want to service on or off, click **OK** to make each channel's new target state its current state.

Service On/Off

Use this window to set service on or off for channel paths. Set service on and off to control whether the channel paths are on standby in, or reserved from, the active input/output (I/O) configuration:

Important: Do not use this window to set service on or off unless you have been directed to do so.

- A channel path is on *Standby* or *Reserved* while service is set off. It is in the active I/O configuration but it cannot be used until it is configured on. It will remain in the active I/O configuration until service is set on.
- A channel path is *Reserved - Service* while service is set on. It is not in the active I/O configuration and cannot be used. It will remain out of the active I/O configuration until service is set off.
- A channel path is *Reserved* while service is set off. It is not in the active I/O configuration. A PCHID can be in a reserved state if it is not defined in the active IOCDS.

Setting service on for a channel path, which removes it from the active I/O configuration, allows running diagnostic tests on the channel path without disturbing other channel paths being used by the system.

Setting service on for a channel path can be used also to remove failing channel paths from the I/O configuration so subsequent power-on resets will not attempt to initialize the filing channel paths.

To use the **Service On/Off** task the CPC must be power-on reset.

The window lists the following information for each channel path you selected to start the task. The information displayed depends on what object is selected. Selecting a crypto shows the Cryptographic number in the first column. Selecting a channel path shows the CSS and CHPID values in the first column. Select one or more channel paths or cryptos, then select **Toggle** from the drop down box to toggle their target states.

PCHID
Displays a four-digit physical channel identifier (PCHID) of each channel path.

"Current State" on page 802
Indicates the current state of each channel path.

Desired State
Indicates the target state of each channel path.

Messages
If you attempt to change the target state of a channel path that cannot have service set on or off, this column displays the message "Not Allowed" for the channel path to indicate that changing its state is not allowed.

Current State

This window lists the current state and target of each channel path you selected to start the task. Use the window actions to *toggle* the target states of the channel paths you want to set service on or off.

- If the current state of a channel path is **Reserved - Service** toggle its target state to **Standby** or **Reserved** if you want to set service off for the channel path.
- If the current state of a channel path is **Standby,** or **Reserved** toggle its target state to **Reserved - Service** if you want to set service on for the channel path.

Online
Indicates the channel path is configured on. It is in the active Input/Output (I/O) configuration and it can be used. Service cannot be set on for the channel path until it is configured off.

Online pending
When the Central Processor Complex (CPC) is activated, this state indicates the channel path was configured on while assigned to an inactive logical partition. The channel path will be online when the logical partition is activated. Service cannot be set on for the channel path until it is configured off.

Reserved - Service
Indicates the channel path has service set on. It is not in the active I/O configuration, cannot be configured on, and cannot be used. It will remain out of the active I/O configuration until service is set off.

Reserved
Indicates the channel path has service set off. A PCHID can be in the reserved state if it is not defined in the active IOCDS.

Standby
Indicates the channel path has service set off. It is in the active I/O configuration but it cannot be used until it is configured on. It remains in the active I/O configuration until service is set on.

Additional functions on this window include:

OK

When you finish toggling the target states of the channel path, crypto, or FID you want to configure on or off, click **OK** to allow the new target states to take effect.

Cancel

To close the Service On/Off window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Service Required State Query

Service Required State Query

Use **Service Required State Query** to determine the reason for the Service Required State. If a pop up window indicates you are **not** in Service Required State at this time, the system is operating under normal conditions.

The list of reasons for the Service Required State displays only in a Service Required State.

Reasons

The **Service Required State** indicates that the next disruption will result in the system operating in a degraded capacity or will fail.

This window lists reasons that the Support Element is in the Service Required State:

N-Mode Power
The N-Mode Power check determined redundant power is not available for the central processor complex (CPC) and each I/O cage.

Primary Support Element loss of communication with Alternate Support Element
Communication between the Primary Support Element and the Alternate Support Element was lost. The mirroring function will not work and the alternate Support Element may not be up to date.

Memory Sparing Threshold Reached
Reaching the Memory Sparing Threshold will leave the CPC operating in a degraded capacity.

An Oscillator/BMC card is defective
Service is required to replace the card.

The Service Network is in N-mode
A problem was detected in the network that has caused a service required state.

The Alternate SE is fenced
A problem was detected on the Primary Support Element that has caused an auto switch of the Primary Support Element to the Alternate Support Element.

IO domain is in N mode
A hardware failure in the IO domain path to be repaired. When resulting from a previous failed EDA or CDR operation, it is NOT showing a hardware failure in the IO domain path. Instead, the path(s) will be restored to the default paths as soon as the EDA or CDR operation completes successfully.

RAIM memory is degraded
A problem was detected with RAIM memory being degraded.

Redundant service path to a FRU has failed
A hardware failure to a FRU was detected and requires service.

Customer Initiated Power Maintenance
The system is currently in a customer initiated power service state. Some power and service network failures are not reported in this state. Reporting will start after power service state has ended.

Additional functions are available from this window:

OK
To close the window, click **OK**.

Help
To display help for the current window, click **Help**.

Service Status

Accessing the Service Status task

This task sets a system to Service Status allowing a service representative to perform service tasks on the system or Support Element. Many of the system service tasks require that the system is first placed in Service Status. Repair and Verify, for example, cannot be run on a system until that system is placed in Service Status.

Service Status should be enabled for systems that are to be serviced. When in Service Status, the system status displayed on its Details window will be Service and no other status will be reported by the system until Service Status is disabled. During a service action, status changes (for example, No Power) that would normally cause an exception due to an unacceptable status will not cause an exception when the status is Service. System images will not be displayed on the Hardware Management Console when Service Status is enabled for the system.

Service status also prevents messages indicating the loss of communication to the Support Element from displaying while the Support Element is powered off or during licensed internal code (LIC) load.

To set the service status:

1. Select one or more systems.
2. Open the **Service Status** task. The Service Status window is displayed.
3. Select one or more objects from the table to change the status (check marks will appear).
4. Point to **Options** from the menu bar and then click **Enable service status**, **Disable service status**, or **Display error message** to enable or disable service status or display error messages, respectively.
5. Click **Save** to save your changes.
6. When you are asked if you are sure you want to save your changes, click **Yes**.

Service Status

Use this window to set the service status of one or more systems. You can also display error messages about the service status of the systems.

The service status of a system determines whether tasks that disrupt system operations can be performed in the service user mode of the system console or a Hardware Management Console.

Ordinarily, the service status for a system is disabled. This prevents the use of disruptive operations in the service user mode.

A service representative will request you temporarily enable the service status for a system. The service representative will need service status enabled to complete service procedures that may require performing disruptive operations.

To set the service status or to view error messages for a system, select the system or systems from the list, then click **Options** and select an action from the drop-down menu.

Note: The service status settings you change take affect only if you save them. Click **Save** to save changed settings.

Status Table

Object Name
Displays the names of the systems in the group selected.

Service Status
Indicates whether service status for the system is currently enabled or disabled, or if there is a service status error.

Options

Enable service status
To set the service status setting for the selected system to enabled, select **Enable service status**. The setting takes affect when you click **Save**. This setting permits the use of console operations in the service user mode that disrupt system operations.

Disable service status
To set the service status setting for the selected system to disabled, select **Disable service status**. The setting takes affect when you click **Save**. This setting prevents the use of console operations in the service user mode that disrupt system operations.

Display error message
To display a more detailed error message about the service status of the selected system, select **Display error message**.

Additional functions are available from this window:

Save
To save the settings currently displayed for service status, click **Save**.

The **Service Status** column displays the service status settings that will be saved.

Note: You must save changed service status settings to make them take affect.

Reset
To undo changes made to the service status settings and display again the settings most recently saved, click **Reset**.

Note: Click **Cancel** to undo changes made to the service status settings and to exit the task.

Cancel
To undo changes made to the service status settings, and to exit the task and return to the Hardware Management Console Workplace, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Service User Mode

Provides tasks and operations for problem determination and repair. Its intended users are the service representatives of the service provider for a system.

A service user mode is available at any system console or any Hardware Management Console. The access administrator for a console controls the user identifications and passwords that can be used to log in with the SERVICE default user ID or a user ID with service roles.

Enable service status

To enable the service status for one or more systems:

1. Select a system or systems from the names in the table (a checkmark appears in the **Select** column).
2. From the **Options** drop-down menu, select **Enable service status**.

   The **Service Status** column in the table displays **Enabled** to indicate that the service status is enabled for the selected system or systems.
3. To save the settings currently displayed in the list, click **Save**.

   A message panel is displayed verifying you want the setting to be changed.
4. Click **Yes** to save the change, **No** to keep the original setting.

   The **Service Status** window is displayed again.
5. To return to the Hardware Management Console Workplace, click **Cancel**.

Disable service status

To disable the service status for one or more systems:

1. Select a system or systems from the names in the table (a checkmark appears in the **Select** column).
2. From the **Options** drop-down menu, select **Disable service status**.

   The **Service Status** column in the list displays **Disabled** to indicate that the service status is disabled for the selected system or systems.
3. To save the settings currently displayed in the list, click **Save**.

   A message panel is displayed verifying you want the setting to be changed.
4. Click **Yes** to save the change, **No** to keep the original setting.

   The **Service Status** window is displayed again.
5. To return to the Hardware Management Console Workplace, click **Cancel**.

Display error message

To display a more detailed error message about the service status for a systems:

1. Select a system or systems from the names in the table that indicates an error message (a checkmark appears in the **Select** column).
2. From the **Options** drop-down menu, select **Display error message**.

   The **Failure Details** window displays a detailed explanation of the error and what steps should be taken to correct it.
3. Click **OK**.

   The **Service Status** window displays again.
4. To return to the Hardware Management Console Workplace, click **Cancel**.

Set Power Cap

Accessing the Set Power Cap task

This task allows you to limit the peak power consumption of a system resource or group of resources. You can closely manage power allocations within the physical limits of your data center.

The actions you can perform on the system resources from this task include:

- Selecting the Power Capping setting
- Setting the Cap Value
- Viewing power capping details on default and hidden columns

To set the power cap:

1. Open the **Set Power Cap** task. The Set Power Cap window is displayed. The window lists the current power capping settings and power cap values for the object.
2. Select a system.
3. Select the power capping setting from the **Power Capping** drop-down list.
4. Specify the power cap in the **Cap Value (Watts)** field.
5. Click **OK** to complete the task.

Set Power Cap

Use this task to limit the peak power consumption of a system component or group of components. You can closely manage power allocations within the physical limits of your data center.

You can work with the table by using the table icons or **Select Action** list from the table toolbar. If you place your cursor over an icon, the icon description is displayed. The icons and list actions perform the following functions:

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want. Click **OK** when you have defined your filter. The filtered view can be toggled on and off by selecting the check box next to the desired filter in the filter row. If you no longer want the **Filter** row to appear, click **Hide Filter Row**.

Clear All Filters
Returns to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header to change from ascending to descending order. Click **OK** when you have defined your preferred order.

Clear All Sorts
Returns the table back to the default order.

Configure Columns
Allows you to arrange the columns in the table in the order you want or to hide columns from view. All available columns are listed in the Columns list by their column names. You select the columns you want displayed or hidden by selecting or clearing the box next to the column names. Manipulate the column order by selecting a column name in the list and clicking the arrows to the right of the list to change the order of the selected columns. When you have completed the configuration and you want to save the settings, click **OK**. Otherwise, click **Cancel** and your changes will not be saved.

This window displays all components of the system. However, only components that support power capping are enabled. The same window is displayed regardless of how you launch the task. The actions you can perform on the system components include:

- Selecting the Power Capping setting
- Setting the **Cap Value**
- Viewing power capping details on default and hidden columns

The following information is available from the power capping table:

Name
Specifies the name of the object.

Type
Specifies the object type. The types available for power capping depend on your system configuration.

Power Capping
Select the power capping setting for the object from the drop-down list.

Note: This field is disabled and will default to **Not Supported** if power capping is not supported for this object.

Cap Value (Watts)
Enter the current cap value for the object in watts (W). The current cap value indicates the power budget for the selected object and must be within the **Cap Value Range**. This field may be automatically set, if under group capping control. See Group Capping for more information.

Note: This field is disabled if power capping is not supported for this object.

Cap Value Range (Watts)
Specifies the minimum and maximum values for the **Cap Value** in watts (W). This defines the set of acceptable values for setting the power cap. There are special considerations for group capping. See Group Capping for more information.

Last Power Capping
Specifies the current **Power Capping** setting for the object.

Note: This column is hidden by default. Use **Column Configuration** to display this column.

Last Cap Value (Watts)
Specifies the current **Cap Value** for the object in watts (W). The **Last Cap Value** indicates the active power budget for the selected object. When the task is initially opened, this is the same as the **Cap Value**.

Note: This column is hidden by default. Use **Column Configuration** to display this column.

Location
Specifies the location of the object.

Serial
Specifies the serial number of the object.

MTM
Specifies the machine type and model number of the object.

Note: If you are not entitled to access the **Set Power Capping** task, all rows of the table will be disabled.

Additional functions from this window include:

OK
To save the power capping settings for this system, click **OK**.

Apply
To save the power capping settings for this system and continue customization, click **Apply**.

Note: This option is grayed out until a change is made within this window.

Cancel
To close this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Power Capping

Select the power capping setting from the **Power Capping** drop-down list. The possible settings include:

Disabled
The power cap of the object is not set, and the peak power consumption is not limited.

Enabled
The peak power consumption of the object is limited to the current **Cap Value**. When this setting is selected for system objects, all components of the object available for power capping are capped to limit the peak power consumption. Use this setting to enable group capping.

Custom
You can individually configure the components of the object for power capping. You can also use this setting to disable power capping for a system but retain the individual **Power Capping** setting and **Cap Value** for the objects within the system.

Note: This setting is available only for system objects.

For more information on group capping, see Group Capping.

Note: This field is disabled and will default to **Not Supported** if power capping is not supported for this object.

Last Power Capping

Specifies the current power capping setting of the object. When the task is initially opened, this is the same as the **Power Capping** setting. The possible settings include:

Disabled
The power cap of the object is not set, and the peak power consumption is not limited.

Enabled
The peak power consumption of the object is limited to the current **Cap Value**. For system objects, all components of the object available for power capping are capped to limit the peak power consumption.

Custom
You can individually configure the components of the system for power capping.

Note: This setting is available only for system objects.

For more information on group capping, see Group Capping.

Note: This column is hidden by default. Use **Column Configuration** to display this column.

Group Capping

A group is composed of an object that contains another object and the object or objects it contains. For example, a group might be a CPC that contains a zCPC. The following are important concepts regarding group power capping:

- Group caps replace individual object caps--that is, the **Cap Value** of a group supersedes the power cap of any object contained within the group.
- You can enable group capping by setting the **Power Capping** setting of the group to **Enabled**.
- You can change individual **Cap Value**s if the object is under group capping control. Customizing the individual **Cap Value** within a group, will automatically change the **Power Capping** setting to **Custom** for the group.
- If a group contains an object that does not support power capping, the **Power Rating** is used in calculating the minimum power cap value for the group. The **Power Rating** can be found on the details window for an object.
- The maximum **Cap Value** for a group is the sum of the **Power Rating** of all group objects.
- When a group component is powered off or removed, the group cap is redistributed to the remaining group components.
- To disable group capping without changing the individual power caps of the group members, change the **Power Capping** setting of the group to **Custom**.

Set Power Saving

Accessing the Set Power Saving task

This task allows you to reduce the average energy consumption of a system component or group of components. You can closely manage power allocations within the physical limits of your data center.

Note: When the power save mode is active some upgrade options are not available for the **Perform Model Conversion** task.

To set power saving:

1. Open the **Set Power Saving** task. The Set Power Saving window is displayed. The window lists the current power saving settings for the object.
2. Select a system.
3. Specify the power saving setting for the systems resources in the **Power Saving** list
4. Click **OK** to complete the task.

Note: You can set the power saving setting of the zCPC to **Low power** only one time per calendar day. This field is disabled and set to **Not Supported** if the current zCPC power saving setting is **High performance** but the zCPC has already entered **Low power** once within the calendar day.

Set Power Saving

Use this task to reduce the average energy consumption of a system component or group of components. You can closely manage power allocations within the physical limits of your data center.

This window displays all components of the system. However, only components that support power saving are enabled. The same window is displayed regardless of how you launch the task.

The following information is available from the power saving table:

Name
Specifies the name of the object.

Type
Specifies the object type. The types available for power saving depend on your system configuration.

Power Saving
Select the power saving setting for the object.

Note: This field is disabled and will default to **Not Supported** if power saving is not supported for this object.

Last Power Saving
Specifies the last power saving setting for the object. When the task is initially opened, this is the same as the **Power Saving** setting.

Note: This column is hidden by default. Use **Column Configuration** to display this column.

Location
Specifies the location of the object.

Serial
Specifies the serial number of the object.

MTM
Specifies the machine type and model number of the object.

Note: If you are not entitled for the **Set Power Saving** task, all rows of the table will be disabled.

Additional functions are available from this window:

OK
To save the power saving settings for this system, click **OK**.

Apply
To save the power saving settings for this system and continue customization, click **Apply**.

Note: This button is grayed out until a change is made within this window.

Cancel
To close this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Power Saving

Select the power saving setting from the **Power Saving** list. Power saving reduces the energy consumption of a system. The possible settings include:

High performance
The power consumption and performance of the object are not reduced. This is the default setting.

Low power
The performance of the object is reduced to allow for low power consumption. When this setting is selected for system objects, all components of the object enabled for power saving have reduced performance to allow for low power consumption. Use this setting to enable group power saving.

Note: When configuring the power saving setting for systems cooled by forced-air, you can only set the power saving setting of the zCPC to **Low power** one time per calendar day. This field will be disabled and set to **Not Supported** if the current zCPC power saving setting is **High performance** but the zCPC has already entered **Low power** once within the calendar day.

Custom
Use **Custom** to disable group power saving and individually configure the components of the object for power saving.

Note: This setting is available only for system objects.

For more information on group power saving, see Group Power Saving

Note: This field is disabled and set to **Not Supported** for objects that do not support power saving.

Group Power Saving

A group is composed of an object that contains another object and the object or objects it contains. For example, a group might be a CPC that contains a zCPC . The following are important concepts regarding group power saving:

- Group power saving settings replace individual object settings--that is, the **Power Saving** setting of a system supersede the **Power Saving** setting of any object contained within the system.
- You can enable group power saving by setting the **Power Saving** setting of the system to **Low power** or **High performance**.
- You can change individual **Power Saving** settings if the object is under group power saving control. Customizing the individual **Power Saving** settings within a system, will automatically change the **Power Saving** setting to **Custom** for the system.
- To disable group power saving without changing the individual **Power Saving** settings of the group members, change the **Power Saving** setting of the system to **Custom**.

Show LED

Accessing the Show LED task

Show LED is a channel operation you can use to find the location of the jack and card slot in a cage. The light emitting diode (LED) is located below each card slot and near each jack in the cages that support attachment hardware. You can use this task for channel problem determination.

To set the show LED on:

1. Locate the **Channel** or **Channel path** that you want the LED on for.
2. Open the **Show LED** task.

   The Show LED window displays the PCHID for the LED that is on.
3. Click **OK** to turn the LED off.

Start Processor

Accessing the Start Processor task

Follow your local procedures for determining when to start processors. But generally, starting processors for an image is most effective after you've used the **Stop Processor** task to stop processors for the image.

To start processors for an image:

1. Locate the **CPs** you want to start.

2. Open the **Start Processor** task.

   This immediately performs the operation; the processor is started and resumes operating.

Start (DPM)

Accessing the Start task

This task starts a stopped system or partition on which Dynamic Partition Manager (DPM) is enabled.

Note: This task is available on the HMC only when one or more managed systems have DPM enabled.

To start a stopped DPM system or partition:

1. Select a stopped DPM system, or one or more stopped partitions.

   Note: You cannot mix your selection of systems and partitions.

2. Open the **Start** task.

   If the DPM R3.1 storage management feature or a later DPM version has been applied to the system, and one or more of the partitions to be started have attached storage groups that are being configured or modified, a warning message is displayed. The warning message includes the name of the affected partitions. The Start task does not continue until you make a selection.

   - Select **YES** to allow the affected partitions to be started.
   - Select **NO** to cancel the start operation for only the affected partitions.

   The Start window contains the following controls and information.

   Progress bar
   The overall total progress bar shows an aggregated status of all targeted partitions or the progress of the targeted system for this task instance.

   Note: The total system progress bar should be equal to the **Progress** column of the system in the table.

   Table
   Displays a tree-table for a targeted system followed by all the partitions configured to be started automatically with the system, displaying their individual progress. It can also display a list of targeted partitions with the associated system and individual progress. The Actions menu and row menu contain the following items for managing the table:

   Actions menu or toolbar icon
   Use the Actions menu or select an icon on the toolbar for your options.

   Partition Details
   To display the Partition Details window for each selected target, select **Partition Details**. This selection is enabled when one or more rows are selected.

   System Details
   To display the System Details window for the targeted system or each selected target's system (one per CPC), select **System Details**. This selection is enabled when one or more rows are selected.

   Open Console
   To open the **Open ASCII Console** task in a new window for the selected targets, select **Open Console** or click the toolbar icon. This selection is enabled when one or more rows are selected.

   OS Messages
   To open the **Operating System Messages** task in a new window for the selected targets, select **OS Messages**. This selection is enabled when one or more rows are selected.

Retry
To restart this function on the selected targets, which resets the progress, select **Retry** or click the toolbar icon. This selection is enabled when one or more targets that are in a failure state are selected.

Cancel
To cancel this function on the selected targets, removing their progress, select **Cancel** or click the toolbar icon. Initially, **Cancelling** is displayed in the Details column. When the function completes, **Cancelled** is displayed in the Details column. If the cancel fails, then an error message is displayed. This selection is enabled when one or more targets in a cancelable state are selected.

Monitor System
To monitor the system, select **Monitor System** or click the toolbar icon. This option brings the main user interface (UI) to the foreground, select the targets' system from the Navigation area and then select the **Monitor** tab in the work area. **Monitor System** is enabled when one or more targets are selected for the same system, and is disabled if partitions from different systems are selected.

Table columns
A description of the table columns for the systems or partitions follows.

Select
You can select one or more table entries.

Target
Displays the system or partition name as a hyperlink. To open **System Details** or **Partition Details** in a new task window, click the appropriate link.

Partition
Displays the partition name as a hyperlink. To open **Partition Details** in a new task window, click this link.

System
Displays the system name on which the partition resides as a hyperlink. To open **System Details** in a new task window, click this link.

Progress
Displays a progress bar identifying the percentage of progress for partitions waiting to start, partitions in the process of starting, and partitions that have started. The percentage is based on the amount of steps performed on the function and not on the amount of time.

Details
Displays the name of the step currently being performed, or content that describes the outcome of the operation. If the DPM R3.1 storage management feature or a later DPM version has been applied to the system, the Details column contains messages that indicate the outcome. Otherwise, the Details column contains one of the following icons and labels, with a clickable **Details** link that identifies the failed partitions and provides a message that explains the failure.

- **Success** indicates partitions that have started.
- **Failed** indicates partitions that failed to start.
- **Cancelled** indicates partitions for which the start operation was canceled.

Depending on the outcome of the start operation for a partition, additional messages might be displayed in the Details column.

- The **Open Console** link opens the console task through which you can log in to the operating system that is running on the partition.
- The Secure Service Container Web Interface Communication link opens a web browser, using the host name or IP address that is specified for a partition with the type Secure Service Container.
- Only when an administrator has created one or more network interface cards (NICs) with associated VLAN IDs for a new or modified partition, the Details column includes a list of

those network devices. The list includes each NIC device number and the associated VLAN ID to be used when configuring the device on the operating system that the partition hosts.

- If the message Maximum Number of Partitions is displayed, the storage groups that are attached to the started partition are already in use by the maximum number of active partitions. This message means that storage is not available for the partition to use. In this case, go to the Storage section of the **Partition Details** task, and attach more storage groups to the partition.
- If the message No Boot Volume is displayed, an operating system or hypervisor cannot be started on this partition. In this case, go to the Storage section of the **Partition Details** task, and attach a storage group that contains a boot volume on which the executables for the operating system or hypervisor reside.

Close

When the task is complete, click **Close**. This option is not enabled until all the targets reach their final state of this function, which is either a failure, canceled, or 100% completed.

Note: In the case of a retry on a failed target, the close option is disabled again if it became enabled. If you click the task window's red X, the window either reopens to its current state if it is not completed or closes the task if it is completed.

3. When you complete this task, click **Close**.

Start All Processors

Accessing the Start All Processors task

Follow your local error recovery procedures for determining when to start all processors. Generally, starting all processors for an image is most effective after you have used the **Stop All Processors** task to stop all processors for the image.

To start all processors for an image:

1. Locate the **Image** you want to work with.

   Note: Stopping an image can be considered disruptive. If the image is locked, unlock it.

2. Open the **Start All Processors** task to start all processors for the image.

   This immediately performs the operation; all processors for the image are started and resume operating.

Stop Processor

Accessing the Stop Processor task

Follow your local procedures for determining when to stop processors. Generally, stopping processors for an image is effective only when the image and processors are operating.

To stop processors for an image:

1. Open the **Stop Processor** task.

   This immediately performs the operation; the processor is stopped.

Stop (DPM)

Accessing the Stop task

This task stops a started system (or partitions) on which Dynamic Partition Manager (DPM) is enabled.

Notes:

- This task is available only when one or more managed systems have DPM enabled.
- Stop is considered a disruptive task. If the target is locked, you must unlock it before continuing.

To stop a started DPM system or partition:

1. Select a started DPM system, or one or more started partitions.

   Note: You cannot mix your selection of systems and partitions.

2. Open the **Stop** task. The "Confirm Disruptive Action" on page 816 window is displayed. When you have agreed to continue with the task, the Stop window is displayed. The details of the window include the following information:

   Progress bar
   The overall total progress bar shows an aggregated status of all targeted partitions or the progress of the targeted system for this task instance.

   Note: The total system progress bar should be equal to the **Progress** column of the system in the table.

   Table
   Displays a tree-table for a targeted system followed by all the partitions configured to be started automatically with the system, displaying their individual progress. It can also display a list of targeted partitions with the associated system and individual progress. The Actions menu and row menu contain the following items for managing the table:

   Actions menu or toolbar icon
   Use the Actions menu or select an icon on the toolbar for your options.

   Partition Details
   To display the Partition Details window for each selected target, select **Partition Details**. This selection is enabled when one or more rows are selected.

   System Details
   To display the System Details window for the targeted system or each selected target's system (one per CPC), select **System Details**. This selection is enabled when one or more rows are selected.

   Cancel
   To cancel this function on the selected targets, removing their progress, select **Cancel** or click the toolbar icon. Initially, **Cancelling** is displayed in the Details column. When the function completes, **Cancelled** is displayed in the Details column. If the cancel fails, then an error message is displayed. This selection is enabled when one or more targets in a cancelable state are selected.

   Monitor System
   To monitor the system, select **Monitor System** or click the toolbar icon. This option brings the main user interface (UI) to the foreground, select the targets' system from the Navigation area and then select the **Monitor** tab in the work area. **Monitor System** is enabled when one or more targets are selected for the same system, and is disabled if partitions from different systems are selected.

   Table columns
   A description of the table columns for the systems or partitions follows.

   Select
   You can select one or more table entries.

   Target
   Displays the system or partition name as a hyperlink. To open **System Details** or **Partition Details** in a new task window, click the appropriate link.

   Partition
   Displays the partition name as a hyperlink. To open **Partition Details** in a new task window, click this link.

   System
   Displays the system name on which the partition resides as a hyperlink. To open **System Details** in a new task window, click this link.

Progress
Displays a progress bar identifying the percentage of progress for partitions waiting to stop, partitions in the process of stopping, and partitions that have stopped. The percentage is based on the amount of steps performed on the function and not on the amount of time.

Details
Displays the name of the step currently being performed, or content that describes the outcome of the operation. If the DPM R3.1 storage management feature or a later DPM version has been applied to the system, the Details column contains messages that indicate the outcome. Otherwise, the Details column contains one of the following icons and labels, with a clickable **Details** link that identifies the failed partitions and provides a message that explains the failure.

- **Success** indicates partitions that have stopped.
- **Failed** indicates partitions that failed to stop.
- **Cancelled** indicates partitions for which the stop operation was canceled.

Close
When the task is complete, click **Close**. This option is not enabled until all the targets reach their final state of this function, which is either a failure, canceled, or 100% completed.

Note: In the case of a retry on a failed target, the close option is disabled again if it became enabled. If you click the task window's red X, the window either reopens to its current state if it is not completed or closes the task if it is completed.

3. When you complete this task, click **Close**.

Confirm Disruptive Action

This window is used to confirm that you want to stop a started system or partition. If a system is targeted, this window displays any partitions on the system that are not stopped; otherwise, this window displays the targeted partitions.

Note: If necessary, you might be required to provide confirmation text input for each object and you might also be required to provide your password. These additional requirements ensure that you want to continue with the disruptive task.

The following information is provided in this table:

Name
Specifies the name of the system or partition that is being disrupted by the **Stop** task that is being executed. This name is displayed as a hyperlink. You can click the name to open the Partition Details window.

System
Specifies the system that is associated with the disrupted partition. This name is displayed as a hyperlink. You can click the system to open the System Details window.

Status
Specifies the status of the disrupted partition.

OS Name
Specifies the associated operating system name that is associated with the disrupted partition.

Confirmation Text
Provide the operating system name (**OS Name**) (preferred, if available) or the **Name** as input to the **Confirmation Text** fields. You can type the name in the field or copy the name from the table and paste it into the input area. If the confirmation text requirement is disabled for your user ID, then this field is not displayed.

Password confirmation input
Use this input field to specify your user ID password to continue with the disruptive task.

Note: If your user ID does not require a password to continue with the disruptive task, then this input field is not available.

Proceeding with a disruptive task can have severe effects. You are required to confirm the execution of the task by specifying your user ID password in this input field. When you provide the correct password, then **Stop System** or **Stop Partitions** is enabled and you can proceed with the disruptive task.

Some additional functions on this window include:

Stop System (or Partitions)
To proceed with this disruptive action, click **Stop System** or **Stop Partitions**.

Cancel

- To close the window without saving any changes and cancel the stop operation, click **Cancel**.
- If the changes you made did not get saved, a confirmation window opens. Click **Yes** to continue or **No** to return to the previous window.

Help
To display help for the current window, click **Help**.

Stop All Processors

Accessing the Stop All Processors task

Follow your local error recovery procedures for determining when to stop all processors. Generally, stopping all processors for an image is effective only when the image and its processors are operating.

To stop all processors for an image:

1. Locate the **Image** you want to work with.

   Note: Stopping an image can be considered disruptive. If the image is locked, unlock it.
2. Open the **Stop All Processors** task to stop all processors for the image.

   This immediately performs the operation; all processors for the image are stopped.

Stop Processor on CP Address Match

Accessing the Stop Processor on CP Address Match task

The processing and input/output (I/O) activity of central processors (CPs) is reflected in how the activity affects the contents of main storage, the status of I/O devices, and the contents of program status word (PSW). That is, CP activity is indicated by the conditions of main storage, I/O devices, and the PSW.

Monitoring these conditions provides another means for monitoring and controlling CP activity. By setting an *address match* or *event* that identifies the specific condition you want to watch for, all CPs are automatically stopped when the actual condition of main storage, I/O devices, or the PSW matches the condition you set. You can set the following condition for stopping CPs:

CP address match
Set for monitoring main storage and stopping all CPs when a CP accesses a specific main storage location while processing non-I/O operations.

Follow your local procedures for determining when to set conditions for stopping CPs. You can use the Support Element workplace to set conditions for stopping CPs.

To set conditions for stopping CPs:

1. Open the **Stop on Processor CP Address Match** task.

   The window displays controls for setting the conditions that you want to stop the CP.

CP Address Match controls

Use this window to set a condition for stopping all processors when main storage is accessed by a CP at a particular location.

When *Match Active*, *Primary Compare Settings*, and optionally 2 sets of *Secondary Compare Settings* are specified, this function monitors main storage accesses and stops all CPs.

Notes:

1. Only one address match may be active in a system running in Logically Partitioned (LPAR) mode. You can determine which partition has an active address match by looking for the test indicator on the partition status line. If an address match is active for the partition, then the test indicator is shown.
2. If an address match is active in a partition of a system running in Logically Partitioned (LPAR) mode, then the address match is active for every logical processor defined in the partition and all of these logical processors are stopped when the match condition occurs. If the system is not running in LPAR mode, then the address match is active for every physical processor and all of these physical processors are stopped when the match condition occurs.
3. Primary and secondary logical data compare are performed using the then current logical address specification in the PSW (PSW bit 5 (DAT), PSW bits 16-17 (AS)). In AR-mode (DAT=1, AS=01) when GPR x (x not 0) is specified, the AR x to GPR x is used for addressing the data. When GPR 0 is specified, the data is fetched from the primary address space.
4. Data compares are always performed after completion of the unit of operation of the instruction which causes the primary address match by re-fetching the data for the compare. This means that instructions which change the address space (for example, LPSW, LCTL,..) or change the data (for example, MVC, MVCL,...) may not result in a match condition because of the address space switch or because of the changed intermediate data.

Controls

To set the condition, select **Match Active**, specify the Primary Compare Settings, and optionally specify up to 2 sets of Secondary Compare settings.

When an address match is set up for an LPAR partition, then the **Ignore Guest** option means that access to the specified memory should be ignored if they come from a guest of that partition. That is SIE guest 2 accesses should be ignored.

When an address match is set up for the native host system, then the **Ignore Guest** option means that access to the specified memory should be ignored if they come from a guest. That is, SIE guest 1 accesses should be ignored.

The **PASN Compare** option specifies that the match should occur only if the PASN (Primary Address Space Number) in CR 4 bits 16-31 matches the specified **ASN** (Address Space Number).

Primary Compare Settings

One or two secondary compare settings may also be specified. If specified, then the specified conditions are examined each time the primary compare settings are satisfied. A match occurs only when the primary compare settings and all specified secondary compare settings are true.

The types of access to main storage are:

Store Logical
Select this access type to stop all CPs when data is stored by a CP using a logical address which matches that specified.

Icntr Reference Logical
Select this access type to stop all CPs when any CP references the specified logical address to retrieve an instruction.

If the Match Type is set to **Equal**, then a match occurs when the actual data at the specified address logically ANDed with the **Mask** is equal to the specified **Data** logically ANDed with the **Mask**. If the Match Type is set to **Not equal**, then a match occurs when the actual data at the specified address logically ANDed with the **Mask** is not equal to the specified **Data** logically ANDed with the **Mask**. If the Match Type is set to **Not equal**, then a match occurs when the actual data at the specified address logically ANDed with the **Mask** is not equal to the specified Data logically ANDed with the **Mask**.

Additional functions on this window include:

Apply
To save changes made without closing the window, click **Apply**.

Refresh
To update the window with the current changes, click **Refresh**.

Reset
To return the changed values to the previous saved values, click **Reset**.

Cancel
To close the window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Storage Information

Accessing the Storage Information task

The model of your system determines the minimum, standard, and maximum storage capacity of the central processor complex (CPC).

Total Installed storage is part of the CPC's hardware configuration; it is provided by one or more storage cards physically installed in the CPC. *Allocated storage* is installed storage that is in use for a specific purpose:

- The *Customer Storage* is storage amount that is available to your system.
- The *Hardware System Area (HSA)* is storage only the CPC can use. It stores the CPC's licensed internal code and input/output (I/O) definition while the CPC is activated.
- *Virtual Flash Memory* is main memory.
- *Central Storage* includes main storage and internal disk subsystem cache. Operating systems and applications can use main storage; only the CPC can use the cache.

Storage is allocated to a CPC when it is activated.

When the CPC is activated, much of the storage allocated to the CPC can be allocated to the logical partitions activated on it:

- The central storage allocated to the CPC is the central storage initially available to logical partitions.
- The virtual flash storage allocated to the CPC is the virtual storage initially available to logical partitions.

Like the CPC, storage is allocated to a logical partition when it is activated. So to allocate storage to the CPC or a logical partition, you must customize the activation profile you use to activate it.

To review the current storage allocations:

1. Open the **Storage Information** task.
   - Page tabs along the top of the window identify its pages. Select a page tab to display that page.
   - The first page of the window displays information about storage installed and allocated for the CPC. Its page tab is labeled: Base System Storage Allocation.
   - If the CPC is activated, the window includes a second tab that displays information about storage allocated for logical partitions currently activated on the CPC. Its page tab is labeled: Logical Partition Storage Allocation.

Storage Information

This window displays:

- Information about storage installed and allocated for the base system.
- Information about central storage and virtual flash memory storage allocated for logical partitions currently activated on the base system.

Information about storage installed and allocated for the base system and central storage allocated for activated logical partitions is displayed in the tabbed views.

Base system storage allocation
Displays information about storage installed and allocated for the base system.

Logical partition storage allocation
Displays information about central storage and virtual flash memory allocated for logical partitions currently activate on the base system.

Additional functions on this window include:

OK
To close the window, click **OK**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Base System Storage Allocation

Use this window to view the storage configuration information for the central processor complex (CPC). This storage information reflects what is currently allocated.

Total Installed Storage

Displays the amount of storage, in megabytes, that is installed. The installed storage is the total of central storage plus customer storage.

Customer Storage
Displays the amount of storage, in megabytes, allocated for main storage..

Hardware System Area (HSA)
Displays the amount of memory reserved for the base hardware system area (HSA).

Virtual Flash Memory (VFM)

Entitled
Displays the amount of Virtual Flash Memory that is allowed for your system. Entitled Virtual Flash Memory is the amount of Virtual Flash Memory that is licensed for use, which might be less than the total amount that is installed on the system.

Allocated
Displays the amount of Virtual Flash Memory that is allocated, which is the total Virtual Flash Memory assigned to all active and reserved partitions on the system.

Customer Storage Details

Storage Type

Central Storage
Displays the amount of storage, in megabytes and percentage, allocated for main storage and the hardware system area.

Available Storage

Available Storage is the amount of storage initially available to logical partitions. When the CPC is activated, available storage is the amount of storage allocated to the CPC *excluding* the amount allocated for the CPC's hardware system area (HSA). Afterward, the amount of available storage:

- Decreases whenever an inactive logical partition is activated.
- Decreases whenever unused storage is dynamically reconfigured *ON* to a logical partition for which the storage was reserved.
- Increases whenever unused storage is dynamically reconfigured *OFF* from a logical partition for which the storage was reserved.

- Increases whenever an active logical partition is deactivated.

Logical Partition Storage Allocation

This page displays information about central storage and Virtual Flash Memory allocated for logical partitions currently activated on the base system.

The *Base System* is the central processor complex (CPC). When the CPC is activated in LPAR mode, the input/output configuration data set (IOCDS) used to define the CPC's input/output (I/O) definition also identifies the logical partitions that can be activated on the CPC.

When logical partitions are activated, their central storage and Virtual Flash Memory are allocated from the CPC's available storage.

Available Storage is the amount of storage initially available to logical partitions. When the CPC is activated, available storage is the amount of storage allocated to the CPC *excluding* the amount allocated for the CPC's hardware system area (HSA). Afterward, the amount of available storage:

- Decreases whenever an inactive logical partition is activated.
- Decreases whenever unused storage is dynamically reconfigured *ON* to a logical partition for which the storage was reserved.
- Increases whenever unused storage is dynamically reconfigured *OFF* from a logical partition for which the storage was reserved.
- Increases whenever an active logical partition is deactivated.

Input/Output configuration data set (IOCDS)
Displays the identifier and name of the IOCDS used during power-on reset to define the CPC's I/O definition and to identify the logical partitions that can be activated on the CPC.

Central Storage Allocation (MB)

Displays information about how addressable central storage is used for storage allocated to logical partitions currently activated on the central processor complex (CPC). All storage amounts are displayed in megabytes (MB).

Central storage is main storage that operating systems or applications can use. The central storage allocated to a logical partition upon activation is its *initial central storage*. If a logical partition supports dynamic storage reconfiguration, additional central storage reserved for it upon activation is its *reserved storage*. Afterward, if the reserved central storage is not already being used by another logical partition, it can be dynamically reconfigured to the logical partition.

The amounts of initial and reserved central storage are set in the activation profiles used to activate the logical partitions. The storage is also arranged according to information in the activation profiles.

The central storage allocation changes with each activation and deactivation of a logical partition, and whenever unused storage is dynamically reconfigured.

Name
Displays the logical partition's name.

Origin
Displays the offset, from the beginning of central storage addressability, at which central storage for the logical partition begins.

Note: The origin is an offset, *not* an address. So a central storage origin of 2048 MB, for example, indicates the logical partition's central storage addressability begins 512 megabytes from the beginning of central storage addressability.

Initial
Displays the amount of central storage allocated to the logical partition during the most recent activation.

Current
Displays the amount of central storage currently allocated to the logical partition.

If the logical partition supports dynamic storage reconfiguration, this amount is the sum of its initial central storage and any amounts dynamically reconfigured to it from its reserved storage.

Otherwise, this amount is always the same as the initial storage amount.

Maximum
Displays the maximum amount of central storage that can be allocated to the logical partition.

If the logical partition supports dynamic storage reconfiguration, this amount is the sum of the initial central storage and reserved central storage allocated to the logical partition during the most recent power-on reset.

Otherwise, this amount is the same as the initial central storage amount.

Gap
Displays the amount of unused central storage addressability between the end of the central storage addressability for one logical partition and the beginning of the central storage addressability for the next logical partition.

The unused storage may end either at the beginning of central storage allocated to another logical partition, or at the end of central storage.

Virtual Flash Memory (GB)

Name
Displays the logical partition's name.

Initial
Displays the amount of Virtual Flash Memory allocated to the logical partition during the most recent activation.

Current
Displays the amount of Virtual Flash Memory currently allocated to the logical partition element.

Maximum
Displays the maximum amount of Virtual Flash Memory currently allowed for the logical partition.

Store Status

Accessing the Store Status task

Store status is a processor operation you can use to store the contents of a processor's registers, excluding the time-of-day (TOD) clock, in assigned storage locations. The contents of the following registers are stored by the store status operation:

- CPU timer
- Clock comparator
- Current program status word (PSW)
- Access registers 0-15
- Prefix
- Floating point registers 0-6
- General registers 0-15
- Control registers 0-15

If you have experience using other systems, you may have used a store-status key to initiate the store status operation for a processor.

Follow your local procedures for determining when to perform the store status operation. You can use the Support Element workplace to perform the store status operation for any eligible processor. Eligible processors include:

- Physical processors that support the image of a central processor complex (CPC).

- Logical processors that support the images of logical partitions activated in operating modes other than coupling facility mode.

To perform the store status operation:

1. Locate the **CPs** you want to work with.
2. Start the **Store Status** task.

   A message displays when it is completed.
3. Click **OK** to close the message when the operation completes successfully.

   Otherwise, if the operation does not complete successfully, follow the directions in the message to determine the problem and how to correct it.

Swap Channel Path

Swap Channel Path

Swap channel path switches the physical channel identifiers (PCHIDs) associated with a pair of physical channels. To use the **Swap Channel Path** task:

- Put the PCHIDs you want to swap in the Reserved state.
- Select the two PCHIDs from the window. You can only swap ESCON (CVC, CNC, and CTC) FICON (including FCP), and ISC channel types.
- Click **OK**.
- When the operation completes, a status of **Swapped** displays for the selected PCHIDs.

This operation does not apply to internal disks.

A channel path that is swapped may not be swapped again until it is restored to the original status. Use the **Reset Swap Channel Path** task to restore the swapped channel path to the original status. After you reset the swapped channel path, you can swap it with another channel path.

Channel path swapping is used for channel problem isolation. A channel path swap usually is performed with a corresponding physical swap of channel cables. The operation provides a means of redirecting I/O operations from one swapped channel path to the other, without actually changing the I/O configuration defined to the operating system.

Note: Refer to "Channel Swap Procedure" in the *zEnterprise EC12 Service Guide*, GC28-6915.

OK
To swap the channel paths of the selected channels, click **OK**.

Cancel
To cancel the swapping of the selected channels, click **Cancel**.

Help
To display help for the current window, click **Help**.

System Details

Accessing the System Details task

Use this task to view or modify the properties of a system.

Perform the following steps to display and optionally modify the System details:

1. Select the system, and then open the **System Details** task. The System Details window is displayed.
2. Modify the editable fields as you want.
3. Click **Apply** to save the changes.

System Details

This window displays the following information for the selected central processor complex (CPC):

- Instance Information includes the current status of the central processors (CPs) and channels of the CPC and other information about the operating conditions, characteristics, and settings of the CPC.

  Review the information under **Instance information**. Optionally, click **Change Options...** to change the activation profile used for activating the CPC from the group specified in the Group field.
- Acceptable CP/PCHID Status settings determine which CPC, CP, and channel statuses are acceptable. The Support Element reports when the CPC, CP, and channel status becomes unacceptable.

  Review the settings on the **Acceptable Status** page. Optionally, make setting selections, and click **Apply** to change the acceptable status settings.
- Product Information is assigned to machines and CPCs when they are manufactured, primarily for the purpose of identifying them.
- STP Information displays the Server Time Protocol (STP) information for the CPC.

  Note: This tab is available only when STP is enabled and the selected CPC is in an operating state.
- Degrade Reasons indicates the CPC has a degraded status.

  Note: This tab is available only when an object is in a degraded state.
- Busy Status specifies the reason the CPC object is busy.

  Note: This tab is available only when an object is busy.
- Security ("Security" on page 836) to enable BCPii permission settings for the system.

This window also displays product information about the CPC and the machine in which it is located. A *machine* is a particular configuration of hardware designed to provide particular operational capabilities and characteristics.

Additional functions on this window include:

OK
To save changes you made to the acceptable status settings of the system and close the window, click **OK**.

Apply
To save changes you made to the acceptable status settings of the system, click **Apply**.

Change Options...
To change the activation profile used for activating this instance of the CPC from the selected group, click **Change Options**. You can have different activation profiles set for a single system by opening the **System Details** task from different system defined or user-defined custom groups containing the object and selecting **Change Options...**.

The **Change Options...** button is not available if the **System Details** task is invoked from Tasks Index. It is also not available if the user does not have permission to the **Change Object Options** task. Your access administrator can grant permission to the **Change Object Options** task by using the **User Management** task.

Cancel
To close the window without saving changes you made to the acceptable status settings of the system, click **Cancel**.

Help
To display help for the current window, click **Help**.

Instance Information

This page displays the current instance information for the central processor complex (CPC).

Instance Information includes the current status of the central processors (CPs) and channels of the CPC and other information about the operating conditions, characteristics, and settings of the CPC.

“CP status” on page 826
This field displays the current status of the central processor complex (CPC) or a summary of the statuses of its central processors (CPs).

“Channel status” on page 827
This field displays a summary of the statuses of channels that have physical channel identifiers (PCHIDs) defined in the input/output (I/O) configuration of the central processor complex (CPC).

Activation profile
More than one group can contain a unique instance of the same CPC; this situation allows assigning different activation profiles to different instances of the CPC.

Note: The Group field is blank if the **System Details** task is invoked from the Tasks Index.

Last used profile
Identifies the activation profile used for the most recent CPC activation.

Service state
This field indicates whether service status is enabled or disabled for the central processor complex (CPC).

Ordinarily, service status is disabled. But when it is enabled, tasks that might disrupt CPC operations can be performed in the service user mode of the Support Element console of the CPC or any Hardware Management Consoles to which the CPC is defined.

“Alternate SE status” on page 829
This field displays the status of the alternate Support Element (alternate SE) for the central processor complex (CPC).

IOCDS identifier
Displays the identifier of the input/output configuration data set (IOCDS) used during the most recent power-on reset to define the I/O configuration of the CPC.

IOCDS name
Displays the name of the input/output configuration data set (IOCDS) used during the most recent power-on reset to define the I/O configuration of the CPC.

System mode
Identifies the operating mode established for the CPC by the most recent power-on reset.

Number of CPs
Displays the maximum number of Central Processors (CPs) that the CPC supports.

Number of ICFs
Displays the maximum number of Integrated Coupling Facility processors (ICFs), if any, that the CPC supports.

Number of IFLs
Displays the maximum number of Integrated Facilities for Linux processors (IFLs), if any, that the CPC supports.

Number of zIIPs
Displays the maximum number of z Integrated Information Processors (zIIPs) if any, that supports the CPC.

“Dual AC power maintenance” on page 830
This field displays the status of the dual AC power cords of the system.

CP Assist for Crypto functions
Displays whether the Cryptographic CP Assist feature is installed.

Note: If the CP Assist feature is not installed, some functions of the Integrated Cryptographic Service Facility (ICFS) might fail. See the *ICSF Application Programmer's Guide* or the *ICSF System Programmer's Guide* for complete information.

Secure Execution for Linux
Indicates whether the IBM Secure Execution for Linux feature is enabled on the system.

Click **Manage** to import the required global key or host key bundle,view the hashes for the existing global key or host bundle, or clear the secondary global key or host key bundle. You can only import one key bundle at a time from a file system or from an FTP server. For the FTP server option, you need to supply a host name, user name, password, and protocol FTP, FTPS, or SFTP.

Note: This function is only available in the SERVICE user ID or an ID with equivalent permissions. The SYSPROG user ID or an ID with equivalent permissions can only view the hashes for the existing key bundles or clear the secondary key bundles.

"Lock out disruptive tasks" on page 830
Sets the disruptive task lockout for the CPC.

Validated boot certificates
The Certificates table displays the imported certificates assigned to the partitions. If there are no certificates, *No certificates have been installed* displays.

Energy Management

Power rating:
Specifies the maximum power draw of this CPC in watts (W) and Btu/hr. This is a calculated value as indicated by the electrical rating labels or system rating plates of the CPC components.

Power consumption:
Specifies the current power consumption in watts (W) and Btu/hr. for this CPC.

Primary Licensed Internal Code security mode
Displays the Licensed Internal Code security mode for the Primary Support Element (starting on Version 2.14.0). The mode was set using the **Customize Console Services** task.

Alternate Licensed Internal Code security mode
Displays Licensed Internal Code security mode for the Alternate Support Element (starting on Version on 2.14.0). The mode was set using the **Customize Console Services** task.

You can find more detailed help on the following elements of this page:

CP status

This field displays the current status of the central processor complex (CPC) or a summary of the statuses of its central processors (CPs).

Check stopped
This field indicates that all CPs are stopped due to machine checks.

No CPs are operating. Automatic error recovery failed or was not attempted.

Exceptions
This field indicates that at least one CP is operating and at least one CP is not operating, but the exact statuses of the CPs vary.

Note: Use the pop-up menu of the CPC to display the CPs and their exact statuses; instructions are provided in the following information.

Loading
This field displays a load is in progress on all CPs.

No CPs are operating yet, but upon successful completion of the load, all CPs will be operating.

No power
This field indicates the CPC power is off.

CPs cannot operate until CPC power is turned on and a power-on reset is performed.

Not operating
If a power-on reset has not been performed: CPs cannot operate until a power-on reset of the CPC is performed.

If a power-on reset was performed: no CPs are operating, but the exact statuses of the CPs vary.

Note: Use the pop-up menu of the CPC to display the CPs and their exact statuses; instructions are provided in the following information.

Operating
This field indicates that all CPs are operating.

Recovering
This field indicates automatic error recovery is in progress on all CPs.

No CPs are operating, but upon successful recovery from the error, CPs return to their previous statuses.

Otherwise, if error recovery is not successful, CPs are check stopped.

Reset active
This field indicates a reset is in progress on all CPs.

Upon successful completion of the reset, CPs are stopped. No CPs are operating yet, but they are ready for loading.

Service Required
This field indicates the CPC is still operating but is using the last redundant part of a particular type. Your CPC is shipped with more than the required number of parts to operate the CPC. You now have only the required number of parts to keep the CPC running. This is a reminder to you and your service representative to make repairs at the earliest possible time before additional parts fail that would make your CPC non-operating.

Status check
This field indicates the CPC is not communicating with the Support Element.

The status of the CPs cannot be determined.

Stepping
The field indicates all CPs are operating, but with their operation rates set to instruction step.

Each CP will be stopped after processing one instruction or one unit of instructions.

Stopped
This field indicates all CPs are stopped.

If a reset completed successfully: no CPs are operating yet, but they are ready for loading.

If all CPs were stopped manually: no CPs are operating, but they can be started again at any time. Use the **Start all** workplace task to start all CPs simultaneously, or use the **Start** task to start CPs individually.

Channel status

This field displays a summary of the statuses of channels that have physical channel identifiers (PCHIDs) defined in the input/output (I/O) configuration of the central processor complex (CPC).

Note: Channel status is not applicable or cannot be determined while any of the following CPC statuses are displayed in the **CP status** field:

- No power
- Not operating (if a power-on reset had not been performed)
- Status check

Channel status:

Acceptable
Indicates all channels are not operating, but their statuses are acceptable.

The exact statuses of the channels vary. Use the menu of the CPC to see the exact status of each channel; instructions are provided in the following information.

Exceptions
Indicates at least one channel is operating, but at least one channel is not operating.

The exact statuses of the channels vary. Use the menu of the CPC to display the channels and their exact statuses; instructions are provided in the following information.

Not operating
Indicates all channels are not operating and their statuses are unacceptable.

The exact statuses of the channels vary. Use the menu of the CPC to display the channels and their exact statuses; instructions are provided in the following information.

Operating
Indicates all channels are operating.

Determining the status of individual channels

Follow these instructions to display the channels of the CPC and their exact statuses:

1. Close the CPC's Details window to return to the CPC work area.
2. Click **Channels** from the menu to display the channels in the work area.

Note: The label below each icon identifies the physical channel identifier (PCHID), state, and status of the channels.

Import Secure Execution Key

Use this window to import the global key or host key bundle to enable Secure Execution on the system. To enable the Secure Execution feature use the Feature on Demand function in the **Perform Model Conversion** task. Importing the key bundles requires logging in to the Support Element using the SERVICE user ID or an ID with equivalent permissions. Select from the source options to import the global key or host key bundle:

Import from USB
To import either the global key bundle or the host key bundle from a USB device, select the available USB Memory Drive from the list. You can import only one key bundle at a time. Click **Refresh** to update the list.

Import from FTP server

To import either the global key bundle or the host key bundle from an FTP server, complete the following steps. You can import only one key bundle at a time.

Host name
Enter the FTP host name address or destination. This is a required field.

User name
Enter the user name for the target FTP destination. This is a required field.

Password
Enter the password associated with the user name on the target FTP server.

File path
Enter the FTP server directory where files are to be read from.

Protocol
Choose a secure network protocol for transferring files.

FTP
Select this option if you want to use FTP to import a key bundle.

FTPS
Select this option if you want to use the FTP Secure (FTPS) protocol to import a key bundle. FTPS uses the Secure Socket Layer (SSL) protocol to secure data.

SFTP
Select this option if you want to use the Secure File Transfer Protocol (SFTP) to import a key bundle. SFTP uses the Secure Shell (SSH) protocol to secure data.

Additional functions on this window include:

Import
To import the key bundle, click **Import**.

Cancel
To close the window without performing the selected function, click **Cancel.**

Help
To display help for the current window, click **Help**.

Alternate SE status

This field displays the status of the alternate Support Element (alternate SE) for the central processor complex (CPC).

The Support Element you are currently using is the *primary Support Element*. The *alternate Support Element* is the Support Element that is currently not in use. A switch on the frame in which the CPC and its Support Elements are located controls which Support Element is in use (the primary) and which is not (the alternate).

Ordinarily, the primary Support Element remains in use, while the alternate Support Element is operating but idle.

Alternate SE statuses

Back level
Indicates the alternate Support Element is operating but at a lower engineering change (EC) level than the primary Support Element.

Note: To bring the alternate Support Element up to the same EC level as the primary Support Element, you need to make a backup of critical data on the primary Support Element then use it to restore the hard disk of the alternate Support Element. For instructions, see Upgrading a back level alternate Support Element.

None
Indicates the CPC does not have an alternate Support Element installed.

Not operating
Indicates the alternate Support Element is not operating.

Operating
Indicates the alternate Support Element is operating (it is ready to serve as the Support Element of the CPC if you need to switch to it).

Upgrading a back level alternate Support Element

The status of the alternate Support Element's becomes *back level* when, for example, engineering changes (ECs) are installed on the primary Support Element. You can bring the alternate Support Element up to the same EC level as the primary Support Element by using the critical data of the primary Support Element's to restore the hard disk of the alternate Support Element:

1. Log on the Hardware Management Console using the Service Representative default user ID or a user ID with service representative roles.
2. Open a group that contains the CPC of the Support Element.
3. Start the **Backup Critical Data** task on the CPC (the task is available in the **Service** task list).

   Use the task to make a backup of critical data for the CPC's *primary* Support Element. Refer to the online help of this task for more information while using the task.
4. Start the **Hard Disk Restore** task on the CPC (the task is available in the **Service** task list).

   Use the task to restore the hard disk of the *alternate* Support Element of the CPC. Refer to the online help of this task for more information while using the task.

Dual AC power maintenance

This field displays the status of the dual AC power cords of the system.

The system has two three-phase power cords. Internal power distribution is also redundant for added reliability. If input power is removed from either three-phase cord, the system can continue running on the other cord.

It is possible to do periodic maintenance of room power distribution serving the system if only one of the two cords is turned off at a time. Do this only when all internal power circuits are working normally.

Note: Some of the reliability of redundant power is not in effect when running on only one cord.

Dual AC power cord statuses:

Fully redundant
Indicates all redundant power circuits are working normally. If input power is removed from one power cord, the system can continue to run on the remaining cord without loss of function.

Fault detected
Indicates the redundant power circuits are not working normally for one of the following reasons:

- Input power is missing from one of the two cords.
- Some power component within the system might need service. Call service for maintenance.

Not available
Indicates the redundancy check cannot determine the status for one of the following reasons:

- The central processor complex (CPC) and input/output (I/O) cages of the system are not powered on.
- The redundancy check has determined that there might be single-phase AC powered peripheral units that cannot be automatically checked. Therefore AC power maintenance cannot be performed. Call service for assistance.

Lock out disruptive tasks

Sets the disruptive task lockout for the CPC:

Yes
Locks the CPC to prevent the Support Element from performing disruptive tasks on the CPC.

No
Unlocks the CPC to allow the Support Element to perform disruptive tasks on the CPC.

After making your selection, click **Apply** to make the new settings take effect.

About disruptive tasks and the disruptive task lockout

Some Support Element tasks can be *disruptive*. Performing a disruptive task on the central processor complex (CPC) or an image can disrupt its operations. For example, activating the CPC and loading an image can be disruptive.

Setting **Lock out disruptive tasks** controls whether you can perform disruptive tasks on an object. You can lock an object to prevent accidentally performing disruptive tasks on it and then unlock the object only when you want to perform a disruptive task on it.

Note: When you use the Support Element to set an object's disruptive task lockout, the setting affects only disruptive tasks that are started manually by console operators using the Support Element (locally or remotely) or Web server sessions. The setting does *not* affect disruptive tasks started automatically or from other sources. For example, the setting does not affect tasks started by scheduled operations, by Operations Management commands, or by console operators using the Hardware Management Consoles.

Product Information

This page displays product information about the central processor complex (CPC), the machine in which it is located, and the software model capacity identifiers.

A *machine* is a particular configuration of hardware designed to provide particular operational capabilities and characteristics.

Product Information is assigned to machines and CPCs when they are manufactured, primarily for the purpose of identifying them.

CPC serial
Displays the serial number of the CPC

CPC location

Displays the 4-character device location of the central processor complex (CPC). It identifies the CPC's frame and its location (in EIA units) within the frame.

A CPC location consists of:

- A 1-character frame label.
- A 2-character EIA unit label for the location of the CPC from the bottom of the frame.
- A 1-character EIA unit label for the location of the CPC from the left side of the frame.

For example, CPC location A18A indicates the CPC is located:

- In frame A (**A**18A)
- At the 18th EIA unit from the bottom of the frame. (A**18**A)
- At the first EIA unit from the left side of the frame. (A18**A**)

CPC identifier

Displays the 2-digit hexadecimal number mapped to the device location of the central processor complex (CPC).

Note: The **CPC location** field displays the device location of the CPC.

Machine type - model
Displays the machine type and model number.

Machine serial
Displays the serial number of the machine.

Machine sequence
Displays the sequence number of the machine.

Plant of manufacture
Displays the identifier of the plant where the machine was made.

Product of
Displays the identifier of the manufacturer of the machine.

Model-Capacity identifier
Identifies the software model based on all permanent and all temporary active processors on the system.

Model-Temporary-Capacity identifier
Identifies the software model based on the permanent processor capacity plus only the active temporary capacity-based record.

Model-Permanent-Capacity identifier
Identifies the software model based on only the capacity in the permanent processor record

Acceptable CP/PCHID Status

This page displays the current acceptable status settings for the central processor complex (CPC). **Acceptable Status** settings determine which CPC, CP, and channel statuses are acceptable and which statuses are unacceptable. Use the check boxes to change the settings:

- A check mark in a check box indicates an acceptable status.
- An empty check box indicates an unacceptable status.
- To change one setting to the other, clear or select the check box.

The Support Element continuously monitors the statuses of the CPC, CPs, and channels and compares them to the acceptable status settings of the CPC.

You can find the status for the CPC, CP, and channel status in the **Status** column of the work pane table.

Setting the acceptable status settings of the CPC controls which statuses are reported as exceptions:

- Acceptable statuses, indicated by check marks in their check boxes, are *not* reported as exceptions.
- Unacceptable statuses, indicated by empty check boxes, are reported as exceptions.

Operating

This term indicates the status of the central processor complex (CPC) or the summarized status of its central processors (CPs) and channels.

CPC or summarized status of CPs: All CPs are operating.

Summarized status of channels: All channels are operating.

Service

To indicate that a state where CPs are in service status is an acceptable status for the CPC, select **Service**.

A console operator enabled service status for the CPC (ordinarily done at the request of a service representative to allow providing service for the CPC).

Power save

To indicate that utility power for the CPC failed, and one or more of its active control programs put the CPC in a power save state is an acceptable status for the CPC, select **Power save**.

The CPC is using only enough power from its alternate, temporary power source to preserve data for the control programs that put it in the power save state.

Not operating

This term indicates the status of the central processor complex (CPC) or the summarized status of its central processors (CPs) and channels.

CPC or summarized status of CPs:

- If a power-on reset has not been performed: CPC power is on, but its CPs cannot operate until a power-on reset of the CPC is performed.
- If a power-on reset was performed: no CPs are operating, but exact statuses of the CPs vary.
- The following CP statuses are summarized as not operating:
  - Check stopped
  - Loading
  - Recovering
  - Reset active
  - Stepping
  - Stopped

Summarize status of channels:

- Bit error threshold exceeded
- Check stop
- Definition error
- Disabled
- I/O suppressed
- IFCC threshold exceeded
- Loading
- Log stored
- Loss of signal
- Loss of synchronization
- Match
- No power
- Not defined
- Not operational link
- Offline signal received
- Permanent error
- Sequence not permitted
- Sequence time-out
- Service
- Suspended
- Swapped
- Terminal condition
- Test mode
- Wrap block

Note: Each channels settings determine whether the channel statuses are summarized as not operating or acceptable.

Acceptable

This term indicates the summarized status of the channels.

Summarized status of channels: All channels are not operating and their statuses are unacceptable; the exact statuses of the channels vary. The following channel statuses can be summarized as acceptable:

- Bit error threshold exceeded
- Check stop
- Definition error
- Disabled
- I/O suppressed
- IFCC threshold exceeded
- Loading
- Log stored
- Loss of signal
- Loss of synchronization
- Match
- No power

- Not defined
- Not operational link
- Offline signal received
- Permanent error
- Sequence not permitted
- Sequence time-out
- Service
- Suspended
- Swapped
- Terminal condition
- Test mode
- Wrap block

Note: The settings of each channel determine whether the channel statuses are summarized as not operating or acceptable.

Exceptions

This term indicates the status of the central processor complex (CPC) or the summarized status of its central processors (CPs) and channels.

CPC or summarized status of CPs: At least one CP is operating, but at least one CP is not operating.

Summarized status of channels: At least one channel is operating, but at least one channel is not operating.

Service required

This term indicates the status of the central processor complex (CPC) or the summarized status of its central processors (CPs) and channels.

CPC or summarized status of CPs: The CPC is still operating but is using the last redundant part of a particular type. Your CPC is shipped with more than the required number of parts to operate the CPC. You now have only the required number of parts to keep the CPC running. This is a reminder to you and your service representative to make repairs at the earliest possible time before additional parts fail that would make your CPC nonoperational.

No power

This term indicates the status of the central processor complex (CPC) or the summarized status of its central processors (CPs) and channels.

CPC or summarized status of CPs: CPC power is off.

Summarized status of channel paths: This is not applicable to channels.

Degraded

A Degraded status means that, although the CPC is still operating, some hardware is not available.

Status check

The CPC is not communicating with its Support Element.

Save as Default

To change the acceptable status for all of the current objects defined with the same status type, select **Save as default**. After you click **Apply**, a message window is displayed confirming that you want to proceed with this operation.

STP Information

This page displays the current Server Time Protocol (STP) information for the server (CPC).

Note: This tab is available only when STP is enabled and the selected CPC is in an operating state.

Timing state
Specifies the synchronization state of the Time of Day (TOD) clock with respect to the timing network reference time. The possible timing states include:

Synchronized
The server is in this state when the TOD clock is synchronized with the timing network reference time, defined:

- If the server is in ETR timing mode, the server is synchronized with the Sysplex Timer.
- If the server is in STP timing mode, the server is synchronized with Coordinated Server Time (CST).

Unsynchronized
The server is in this state when the TOD clock is not synchronized with the timing network reference time, defined:

- If the server is in ETR timing mode, the server has lost synchronization with the Sysplex Timer.
- If the server is in STP timing mode, the server has lost or has not been able to attain synchronization with CST. The server is out of synchronization with CST when the TOD differs from CST by an amount that exceeds a model dependent STP-sync-check-threshold value.

Stopped
The server is in this state when the TOD clock is either in the stopped state or TOD clock recovery is in progress. After TOD clock recovery completes, the TOD clock enters either the synchronized or unsynchronized state.

Timing mode
Specifies the method by which the TOD clock is maintained for purposes of synchronization within a timing network. The possible timing modes include:

Local
The server is in this mode when the TOD clock has been initialized to a local time and is being stepped at the rate of the local hardware oscillator. The server is not part of a synchronized timing network.

ETR (External Time Reference)
The server is in this mode when the TOD clock has been initialized to the ETR and is being stepped by stepping signals from the ETR. To be in ETR timing mode, the server must be part of an ETR network.

STP (Server Time Protocol)
The server is in this mode when the TOD clock has been initialized to Coordinated Server Time (CST) and is being stepped at the rate of the local hardware oscillator. In STP timing mode, the TOD clock is steered to maintain or attain synchronization with CST. To be in STP timing mode, the server must be part of an STP network.

Timing network [ID]
Specifies the type of timing network in which the CPC is participating and its associated identifier. The network can be Unconfigured, ETR, Mixed CTN (ETR and STP), or STP-only CTN.

Stratum level

Specifies the hierarchy of the server in the timing network. A stratum level 0 indicates that the stratum level is undefined. A stratum level 1 is the highest level in the hierarchy of a timing network that uses STP messages for synchronization. A stratum level 2 server uses STP messages to synchronize to a Stratum 1 server. A stratum level 3 server uses STP messages to synchronize to a Stratum 2 server.

Note: This field is displayed only for a Mixed CTN or an STP-only CTN.

Role of CPC in CTN
Specifies the server roles in a coordinated timing network. The roles include the following:

Note: This field is displayed only for a Mixed CTN or an STP-only CTN.

Preferred Time Server
Is the server you select to be the Preferred Stratum 1 server in an STP-only CTN.

Backup Time Server
Is the server you select to take over as the Current Time Server (Stratum 1 server), because of either a planned or an unplanned reconfiguration.

Current Time Server
Is the server that is currently the Stratum 1 for an STP-only CTN.

Arbiter
Is the server you select to provide additional means for the Backup Time Server to determine if it should take over as the Current Time Server.

Member of the CTN
Is a server that is a member of the CTN but does not currently have a role.

Time zone
Specifies the time zone for this CPC.

Degrade Reasons

A degraded status indicates that, although the CPC is still operating, some hardware is not available. This page indicates why the CPC is in a Degraded status.

Note: This tab is available only when an object is in a degraded state.

Some conditions that can cause the Degraded status include:

- Loss of memory
- Loss of channels due to CPC hardware failure
- Loss of functioning for one or more books
- Open ring connecting the books
- Expiration of capacity backup resources
- Reduced processor frequency due to temperature problem
- IML of CPC during temperature problem.

Busy Status

This page identifies the user ID, the location of the user, and the task that caused the object to become busy.

Security

This page allows you to dynamically enable the Base Control Program internal interface (BCPii) permissions for the system.

Enable the system to receive commands from partitions
To enable the selected system to receive BCPii commands from partitions, select **Enable the system to receive commands from partitions**. When selected, the system can receive BCPii commands from other active logical partitions.

All partitions
Select this option if you want the system to receive BCPii commands from all active logical partition.

“Add partition” on page 837 (Selected partitions)
Select this option if you want to add or remove the logical partitions that are allowed to send BCPii commands to the system.

Add
To add a system and logical partition to BCPii commands to the system, click **Add**.

Remove
To remove a selected logical partition that can send BCPii commands to the system, click **Remove**.

Add partition

Use this window to specify the partitions from which the target system can receive BCPii commands.

Enter system and partition manually
System: Enter the system name for the logical partition from which the target system can receive BCPii commands.

Netid: Enter the Netid name for the selected system.

Partition: Enter the logical partition name from which the target system can receive BCPii commands.

Select a system and partition
System: Select from the drop-down menu the system for the logical partition from which the target system can receive BCPii commands.

Netid: The Netid displays for the selected system.

Partition: Select from the drop-down menu the active logical partition from which the target system can receive BCPii commands.

Additional functions on this window include:

Add
To add the system and partition, click **Add**.

Cancel
To exit the current window without saving changes, click **Cancel**.

System Details (DPM)

Accessing the System Details task

Use this task for information about the selected system that is Dynamic Partition Manager (DPM) enabled.

Note: This task is available on the HMC only when one or more managed systems have DPM enabled.

You can access this task from the main console page by selecting the Systems Management node, by selecting a specific DPM-enabled system, or be selecting this task in the Tasks index. To open the **System Details** task, you must have a customized user ID either with authorization to the task, or with one of the following predefined roles: System Programmer Tasks or Service Representative Tasks. You also can use the default SERVICE user ID, but using a customized user ID is the suggested practice.

To display and optionally modify the details for the selected DPM-enabled system, complete the following steps.

1. Select the system that is DPM-enabled.
2. Open the **System Details** task. The System Details window is displayed.
3. View or modify the editable fields.
4. Click **Apply** to save the changes.

System Details

Use this task to view and manage properties of the selected Dynamic Partition Manager (DPM)-enabled system. To open the **System Details** task, you must have a customized user ID either with authorization to the task, or with one of the following predefined roles: System Programmer Tasks or Service Representative Tasks. You also can use the default SERVICE user ID, but using a customized user ID is the suggested practice.

Use the navigation links to display each tab or use the **Expand All** and **Collapse All** icons to display each section view.

- Select the navigation link or the **Expand** icon to display the "General" on page 838 details tab section.
- Select the navigation link or the **Expand** icon to display the "Status" on page 839 details tab section.
- Select the navigation link or the **Expand** icon to display the "Processors and Memory" on page 844 details tab section.
- Select the navigation link or the **Expand** icon to display the "Adapters" on page 846 details tab section. You can use the Filter function string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.
- Select the navigation link or the **Expand** icon to display the "Management Networks" on page 847 details tab section. You can use the Filter function string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.
- Select the navigation link or the **Expand** icon to display the "Energy" on page 848 details tab section.
- Select the navigation link or the **Expand** icon to display the "Time Server" on page 849 details tab section.
- Select the navigation link or the **Expand** icon to display the "Start Options" on page 850 details tab section.

Note: This task is available on the HMC only when one or more managed systems have DPM enabled.

The navigation pane also includes the following links to related tasks.

System Information
Opens the **System Information** task for the selected system that is Dynamic Partition Manager enabled.

Additional functions on this window include:

OK
To save the current changes and exit the window, click **OK**. The **OK** button is not displayed in view-only mode.

Apply
To save the current changes you made without exiting the window, click **Apply**. The **Apply** button is not displayed in view-only mode.

Cancel
To exit the window, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

General

Use the General details tab section to view the information and modify the description for the selected DPM-enabled system. Use the **Expand All** icon to display the General section. The following list provides a description of each element on the General section.

Name
Specifies the name for the selected system.

Description
Specify an optional meaningful text that describes the selected system. The description can be up to 1024 characters in length.

Object ID
Specifies the associated universal unique identifier (UUID) of the selected system.

Machine type - model
Displays the machine type and model number of the selected system.

Machine serial
Displays the serial number of the selected system.

Machine sequence
Displays the sequence number of the selected system.

Support Element version
Displays the Support Element firmware level of the system.

System mode
Identifies the operating mode established by the most recent power-on reset for the selected system.

CP Assist for Crypto functions
Displays whether the Cryptographic CP Assist feature is installed.

Note: If the CP Assist feature is not installed, some functions of the Integrated Cryptographic Service Facility (ICFS) might fail. See the *ICSF Application Programmer's Guide* or the *ICSF System Programmer's Guide* for more information.

Secure Execution
Indicates whether the required global key and host key for the IBM Secure Execution for Linux feature are installed on the Support Element (SE). This field is displayed only when the feature was ordered, installed, and enabled for this system.

Only when Secure Execution is enabled and your user ID has either the System Programmer Tasks or the Service Representative Tasks role, the General section includes a button through which you can open a separate task to view or manage the keys. **Manage Keys** opens the **Manage Secure Execution Keys** task on the HMC or SE, through which you can view details about each key, including the hashes for the existing global or host key. If your user ID has the System Programmer Tasks role, you can clear the global or host key, which immediately prevents further usage by any partition on the system, and deletes the corresponding key bundle file from the system. If you are logged in to the SE using the SERVICE user ID or an ID with equivalent permissions, you can import the required global key or host key bundle.

Status

Use the Status details tab section to view the current system status and the acceptable status settings for the selected DPM-enabled system. The acceptable status settings determine the system statuses are acceptable or unacceptable. Use the **Expand All** icon to display the Status section. The following list provides a description of each element in the Status section.

Status
Displays a combined current status of the CPC objects for the selected system. If any objects of the CPC are unacceptable, then the overall current status is unacceptable.

CP status
Displays the current status of the system or a summary of the status of its central processors (CPs).

Check stopped
This field indicates that all CPs are stopped due to machine checks.

No CPs are operating. Automatic error recovery failed or was not attempted.

Exceptions
This field indicates that at least one CP is operating and at least one CP is not operating, but the exact statuses of the CPs vary.

Loading
This field indicates that a load is in progress on all CPs.

No CPs are operating yet, but upon successful completion of the load, all CPs will be operating.

No power
This field indicates that the system power is off.

CPs cannot operate until the system is turned on and a power-on reset is performed.

Not operating
If a power-on reset has not been performed: CPs cannot operate until a power-on reset of the system is performed.

If a power-on reset was performed: no CPs are operating, but the exact status values of the CPs vary.

Operating
This field indicates that all CPs are operating.

Recovering
This field indicates that automatic error recovery is in progress on all CPs.

No CPs are operating, but upon successful recovery from the error, CPs return to their previous status values.

Otherwise, if error recovery is not successful, CPs are check stopped.

Reset active
This field indicates that a reset is in progress on all CPs.

Upon successful completion of the reset, CPs are stopped. No CPs are operating yet, but they are ready for loading.

Service Required
This field indicates that the CPC is still operating but is using the last redundant part of a particular type. Your CPC is shipped with more than the required number of parts to operate the CPC. You now have only the required number of parts to keep the CPC running. This field is a reminder to you and your support system representative to make repairs at the earliest possible time before additional parts fail that would make your CPC non-operating.

Status check
This field indicates that the system is not communicating with the Support Element.

The status of the CPs cannot be determined.

Stepping
This field indicates that all CPs are operating, but with their operation rates set to instruction step.

Each CP will be stopped after processing one instruction or one unit of instructions.

Stopped
This field indicates that all CPs are stopped.

If a reset completed successfully: no CPs are operating yet, but they are ready for loading.

If all CPs were stopped manually: no CPs are operating, but they can be started again at any time. Use the **Start all** workplace task to start all CPs simultaneously, or use the **Start** task to start CPs individually.

Alternate SE status

This field displays the status of the alternate Support Element (alternate SE) for the system.

The Support Element you are currently using is the *primary Support Element*. The *alternate Support Element* is the Support Element that is currently not in use. A switch on the frame in which the system and its Support Elements are located controls which Support Element is in use (the primary) and which is not (the alternate).

Ordinarily, the primary Support Element remains in use, while the alternate Support Element is operating but idle.

Back level
Indicates that the alternate Support Element is operating but at a lower engineering change (EC) level than the primary Support Element.

None
Indicates that the CPC does not have an alternate Support Element installed.

Not operating
Indicates that the alternate Support Element is not operating.

Operating
Indicates that the alternate Support Element is operating (it is ready to serve as the Support Element of the system if you need to switch to it).

Channel status

This field displays a summary of the status values of channels that have physical channel identifiers (PCHIDs) defined in the input/output (I/O) configuration of the system.

Note: Channel status is not applicable or cannot be determined while any of the following system status values are displayed in the **CP status** field:

- No power
- Not operating (if a power-on reset had not been performed)
- Status check

Acceptable
Indicates that all channels are not operating, but their status values are acceptable.

The exact status values of the channels vary.

Exceptions
Indicates that at least one channel is operating, but at least one channel is not operating.

The exact status values of the channels vary.

Not operating
Indicates that all channels are not operating and their status values are unacceptable.

The exact status values of the channels vary.

Operating
Indicates that all channels are operating.

Crypto status

Indicates the status of the Crypto Express5S feature card, such as configured, deconfigured, or installed.

Service state

This field indicates whether service status is enabled or disabled for the selected DPM-enabled system.

Ordinarily, service state is disabled. When it is enabled, tasks that might disrupt system operations can be performed in the service user mode of the Support Element console of the system or any Hardware Management Console on which the system is defined.

Dual AC power maintenance

This field displays the status of the dual AC power cords of the system.

Fully redundant
Indicates that all redundant power circuits are working normally. If input power is removed from one power cord, the system can continue to run on the remaining cord without loss of function.

Fault detected
Indicates that the redundant power circuits are not working normally for one of the following reasons:

- Input power is missing from one of the two cords.
- Some power component within the system might need service. Call the support system for maintenance.

Not available
Indicates the redundancy check cannot determine the status for one of the following reasons:

- The system and input/output (I/O) cages of the system are not powered on.

- The redundancy check has determined that there might be single-phase AC powered peripheral units that cannot be automatically checked. Therefore AC power maintenance cannot be performed. Call the support system for assistance.

Degrade reasons

A degraded status indicates that, although the system is still operating, some hardware is not available.

Some conditions that can cause the Degraded status include:

- Loss of memory
- Loss of channels due to a system hardware failure
- Loss of functioning for one or more books
- Open ring connecting the books
- Expiration of capacity backup resources
- Reduced processor frequency due to a temperature problem
- System was IMLed during a temperature problem.

Acceptable CP/PCHID statuses

Use the check boxes to change the settings:

- A check mark in a check box indicates an acceptable status.
- An empty check box indicates an unacceptable status.
- To change one setting to the other, clear or select the check box.

- To the right of the Acceptable CP/PCHID statuses label is a tooltip icon  .

Active

To indicate that the state in which the system is active is an acceptable status for the system, select **Active**.

Acceptable

This term indicates the summarized status of the channels.

Summarized status of channels: All channels are not operating and their status values are unacceptable; the exact status values of the channels vary. The following channel status values can be summarized as acceptable:

- Bit error threshold exceeded
- Check stop
- Definition error
- Disabled
- I/O suppressed
- IFCC threshold exceeded
- Loading
- Log stored
- Loss of signal
- Loss of synchronization
- Match
- No power
- Not defined
- Not operational link

- Offline signal received
- Permanent error
- Sequence not permitted
- Sequence time-out
- Service
- Suspended
- Swapped
- Terminal condition
- Test mode
- Wrap block

Note: The settings of each channel determine whether the channel status values are summarized as not operating or acceptable.

No power

system or summarized status of CPs: system power is off.

Summarized status of channel paths: This is not applicable to channels.

Status check

To indicate that loss of communication is an acceptable status for the system, select **Status check**.

Not operating

This term indicates the status of the central processor complex (system) or the summarized status of its central processors (CPs) and channels.

system or summarized status of CPs:

- If a power-on reset has not been performed: system power is on, but its CPs cannot operate until a power-on reset of the system is performed.
- If a power-on reset was performed: no CPs are operating, but exact status values of the CPs vary.
- The following CP status values are summarized as not operating:
  - Check stopped
  - Loading
  - Recovering
  - Reset active
  - Stepping
  - Stopped

Summarize status of channels:

- Bit error threshold exceeded
- Check stop
- Definition error
- Disabled
- I/O suppressed
- IFCC threshold exceeded
- Loading
- Log stored
- Loss of signal
- Loss of synchronization

- Match
- No power
- Not defined
- Not operational link
- Offline signal received
- Permanent error
- Sequence not permitted
- Sequence time-out
- Service
- Suspended
- Swapped
- Terminal condition
- Test mode
- Wrap block

Note: Each channels settings determine whether the channel statuses are summarized as not operating or acceptable.

Exceptions

To indicate that at least one Central Processor (CP) is operating, but at least one CP is not operating is an acceptable status for the system, select **Exceptions**.

system or summarized status of CPs: At least one CP is operating, but at least one CP is not operating.

Summarized status of channels: At least one channel is operating, but at least one channel is not operating.

Degraded

To indicate that a degraded status where the system is operating but some hardware is not available is an acceptable status for the system, select **Degraded**.

Service required

This term indicates the status of the central processor complex (system) or the summarized status of its central processors (CPs) and channels.

The system is still operating but is using the last redundant part of a particular type. Your system is shipped with more than the required number of parts to operate the system. You now have only the required number of parts to keep the system running. This is a reminder to you and your support system representative to make repairs at the earliest possible time before additional parts fail that would make your system nonoperational.

Processors and Memory

Use the Processors and Memory details tab section to graphically view the system memory and summarize system processors for the selected system that is Dynamic Partition Manager (DPM) enabled. The physical processors can be Central Processors (CP) or Integrated Facility for Linux (IFL). Use the **Expand All** icon to display the Processors and Memory section. The following list provides a description of each element on the Processors and Memory section:

Processors

Indicates the system processor limit, total number of installed physical processors, and the shared and dedicated physical processors on the system. The bar chart scale ranges from 0 to the total amount of physical processors that can be installed on the system. To show the actual number of physical processors that each bar segment represents, hover your cursor over the colored segment.

To the right of the Processor label is a tooltip icon. A dotted line indicates the systems limit and the total number of installed physical processors on the system. To the right of the bar chart, a color legend identifies each segment and values of the bar chart:

System limit
Indicates the system limit size of CPs. It is the maximum number of physical processors that can be installed on the system. The values is represented as a dotted line in the bar chart.

Installed
Indicates the number of physical processors currently installed on the system. This number may be greater than the number of entitled processors. The values are represented as a dotted line in the bar chart.

Shared IFLs
Indicates the number of entitled IFL processors that are not dedicated (the number of physical processors supporting all dedicated virtual IFL processors). If there are no entitled IFL processors, the value is not included in the bar chart.

Dedicated IFLs
Indicates the number of entitled IFL processors that are dedicated (the number of physical processors supporting all dedicated virtual IFL processors). If there are no entitled IFL processors, this value is not included in the bar chart. If there are entitled IFLs, but none are dedicated, this value on the legend is 0.

Shared CPs
Indicates the number of entitled CP processors that are dedicated. (the number of physical processor supporting all shared virtual CP processors). If there are not entitled CP processors, this value is not included in the pie chart.

Dedicated CPs
Indicates the number of entitled CP processors that are dedicated (the number of physical processors support dedicated virtual CP processors). Dedicated amount of CPs dedicated to active and reserved partitions in the system. If there are not entitled CP processors, this value is not included in the pie chart. If there are entitled CPs, but none are dedicated, this value on the legend is 0.

Memory
Indicates the system memory, installed, entitled, and allocated processor memory on the selected system that is Dynamic Partition Manager enabled. The bar chart scale ranges from 0 to the total amount of memory that can be installed on the system. To show the actual amount of allocated memory that each bar segments represents, hover your cursor over the colored segment. To show the actual number of processor memory that each bar segment represents, hover your cursor over the colored segment. To the right of the Memory label is a tooltip icon. A dotted line indicates the systems limit and the total number of installed processor memory on the system. To the right of the bar chart, a color legend identifies each segment and values of the bar chart:

System limit
Indicates the maximum amount of memory that can be installed on the system. The values is represented as a dotted line in the bar chart.

Installed
Indicates the amount of physical memory that can be installed on the system. The values is represented as a dotted line in the bar chart.

Entitled
Indicates the amount of entitled memory for this system. Entitled memory is the amount of memory that is licensed for use, which might be less than the total amount of memory that is installed on the system. The value is represented as a dotted line in the bar chart.

Allocated
Indicates the total amount of allocated memory, which is the total memory assigned to all active and reserved partitions on the system.

Hardware System Area
Indicates the Hardware System Area (HSA) memory reserved for system hardware management.

Model-Capacity identifier
Identifies the software model based on all permanent and all temporary active processors on the selected system that is Dynamic Manager enabled.

Model Temporary-Capacity identifier
Identifies the software model based on the permanent processor capacity plus only the active temporary capacity-based record.

Model Permanent-Capacity identifier
Identifies the software model based on only the capacity in the permanent processor record.

Adapters

Use the Adapters details tab section to view the adapter information for the selected DPM-enabled system. Use the **Expand All** icon to display the General section. The following list provides a description of each element on the Adapters section:

Adapter table toolbar

You can work with the table by using the table icons or **Actions** list from the Adapter table tool bar. If you place your cursor over an icon, the icon description displays.

Configure Options 
Provides a way to exclude or include specific columns from the table display. To configure table options, click the **Configure Options** icon. Available columns are in lists by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**.

Export

Export as HTML
Downloads table data into a Hypertext Markup Language (HTML) file. This action is only available when you are using a remote browser.

Export All to CSV
Downloads table data into a Comma Separated Values (CSV) file. You can then import the downloaded CSV file into most spreadsheet applications. This action is only available when you are using a remote browser.

Print 

Print All
Prints all rows in the table. This action is only available when you are using a remote browser.

Print Selected
Prints selected rows in the table. This action is only available when you are using a remote browser.

Print Preview
Displays a printable version of all rows in the table. This action is only available when you are using a remote browser.

Quick filter
Provides a text area in which you can type a search string to filter the table entries. The table display is limited to only those entries that contain the string in one or more table column values.

Advanced Filter 
Provides advanced filter option through which you can reduce the total number of table entries. To access filter options, click the **Filter** icon.

Columns in the Adapter table

The following columns are displayed for the Adapters table. You can modify the columns in the default table display by using the **Configure Options** icon.

Type
Indicates the adapter type supported on the selected DPM-enabled system.

Number Installed
Indicates the number of adapters installed in your system and configured.

Device Allocation
Displays the current allocation for all adapters (progress bar value, which includes Network Interface Cards (NICs), Host Bus Adapters (HBAs), virtual functions, and usage domains of active and reserved partitions).

Management Networks

Use the Management Networks details tab section displays the current information for the two management interfaces on the selected DPM-enabled system. Use the **Expand All** icon to display the Management Networks section.

Management Networks table toolbar

You work with the table by using the table icons or **Actions** list from the Management Network table tool bar. If you place your cursor over an icon, the icon description displays.

Export

Export as HTML
Downloads table data into a Hypertext Markup Language (HTML) file. This action is only available when you are using a remote browser.

Export All to CSV
Downloads table data into a Comma Separated Values (CSV) file. You can then import the downloaded CSV file into most spreadsheet applications. This action is only available when you are using a remote browser.

Print 

Print All
Prints all rows in the table. This action is only available when you are using a remote browser.

Print Selected
Prints selected rows in the table. This action is only available when you are using a remote browser.

Print Preview
Displays a printable version of all rows in the table. This action is only available when you are using a remote browser.

Standard table functions

The icons perform the following functions in the Management Networks table:

Configure Options 
Provides a way to exclude or include specific columns from the table display. To configure table options, click the **Configure Options** icon. Available columns are in listed by name; choose the columns that you want displayed or hidden by selecting or clearing the items in the list, and then click **OK**

Columns in Management Networks table

The following columns are displayed for the Management Networks table. You can modify the columns in the default table display by using the **Configure Options** icon or action.

Protocol
Identifies the IPv4 or IPv6 address.

Type
Identifies the IPv6 scope.

Mask/Prefix
Displays the TCP/IP subnetwork mask/prefix of the LAN interface.

Primary Support Element IP Address
Displays the TCP/IP address of the LAN interface for IPv4. Displays the universal LAN address and adapter type of the LAN interface (if installed) in the Support Element of the system for IPv6.

Alternate Support Element IP Address
Displays the TCP/IP address of the LAN interface for IPv4. Displays the universal LAN address and adapter type of the LAN interface (if installed) in the Support Element of the system for IPv6.

Energy

Use the Energy details tab section to view the power and thermal monitoring information for the selected DPM-enabled system. Use the **Expand All** icon to display the Energy section. The following list provides a description of each element on the Energy section:

Power rating
Specifies the maximum power draw in watts (W) and Btu/hr of this system. This is a calculated value as indicated by the electrical rating labels or system rating plates of the system components.

Power saving
Specifies the current power saving setting for the system. Power saving reduces the energy consumption of a system and you can manage it using the **Set Power Saving** task. The possible settings include:

High performance
Specifies not reducing the power consumption and performance of the system. This is the default setting.

Low power
Specifies low power consumption for all components of the system enabled for power saving.

Not entitled
Specifies that the server is not entitled for power saving.

Power capping
Specifies the current power capping setting for the system. Power capping limits peak power consumption of a system and, you can manage it using the **Set Power Cap** task. The possible settings include:

Disabled
Specifies not setting the power cap of the system not limiting the peak power consumption. This is the default setting.

Enabled
Specifies capping all components of the system available for power capping to limit the peak power consumption of the system.

Custom
Specifies permitting individual configuration of the components of the system for power capping.

Not supported
Specifies not supporting power capping for this system.

Not entitled
Specifies that the server is not entitled for power capping.

Maximum potential power (W):
Specifies the maximum potential power consumption of a system in watts (W) and Btu/hr. This value is based on the configuration of the system and can be used for power and cooling planning.

Maximum potential heat load (BTU/hr):
Specifies the maximum potential heat load of a system in watts (W) and Btu/hr. This value is based on the configuration of the system and can be used for power and cooling planning.

Time Server

Use the Time Server details tab section to view the current Server Time Protocol (STP) information for the selected DPM-enabled system. Use the **Expand All** icon to display the Timer Server section.

Note: No information is displayed if the STP feature is not installed and enabled on the system.

The following list provides a description of each element on the Timer Server section:

Timing state
Specifies the synchronization state of the time-of-day (TOD) clock with respect to the timing network reference time. The possible timing states include:

Synchronized
The server is in this state when the TOD clock is synchronized with the timing network reference time, defined:

- If the server is in ETR timing mode, the server is synchronized with the Sysplex Timer.
- If the server is in STP timing mode, the server is synchronized with Coordinated Server Time (CST).

Unsynchronized
The server is in this state when the TOD clock is not synchronized with the timing network reference time, defined:

- If the server is in ETR timing mode, the server has lost synchronization with the Sysplex Timer.
- If the server is in STP timing mode, the server has lost or has not been able to attain synchronization with CST. The server is out of synchronization with CST when the TOD differs from CST by an amount that exceeds a model dependent STP-sync-check-threshold value.

Stopped
The server is in this state when the TOD clock is either in the stopped state or TOD clock recovery is in progress. After TOD clock recovery completes, the TOD clock enters either the synchronized or unsynchronized state.

Timing mode
Specifies the method by which the TOD clock is maintained for purposes of synchronization within a timing network. The possible timing modes include:

Local
The server is in this mode when the TOD clock has been initialized to a local time and is being stepped at the rate of the local hardware oscillator. The server is not part of a synchronized timing network.

ETR (External Time Reference)
The server is in this mode when the TOD clock has been initialized to the ETR and is being stepped by stepping signals from the ETR. To be in ETR timing mode, the server must be part of an ETR network.

STP (Server Time Protocol)
The server is in this mode when the TOD clock has been initialized to Coordinated Server Time (CST) and is being stepped at the rate of the local hardware oscillator. In STP timing mode, the TOD clock is steered to maintain or attain synchronization with CST. To be in STP timing mode, the server must be part of an STP network.

Timing network type
Specifies the type of timing network in which the system is participating. The network can be Unconfigured, ETR, Mixed CTN (ETR and STP), or STP-only CTN.

Timing network ID
Specifies the timing network identifier.

Stratum level

Specifies the hierarchy of the server in the timing network. A stratum level 0 indicates that the stratum level is undefined. A stratum level 1 is the highest level in the hierarchy of a timing network that uses STP messages for synchronization. A stratum level 2 server uses STP messages to synchronize to a Stratum 1 server. A stratum level 3 server uses STP messages to synchronize to a Stratum 2 server.

Note: This field is displayed only for a Mixed CTN or an STP-only CTN.

CTN roles
Specifies the server roles in a coordinated timing network. The roles include the following:

Note: This field is displayed only for a Mixed CTN or an STP-only CTN.

Preferred Time Server
Is the server you select to be the Preferred Stratum 1 server in an STP-only CTN.

Backup Time Server
Is the server you select to take over as the Current Time Server (Stratum 1 server), because of either a planned or an unplanned reconfiguration.

Current Time Server
Is the server that is currently the Stratum 1 for an STP-only CTN.

Arbiter
Is the server you select to provide additional means for the Backup Time Server to determine if it should take over as the Current Time Server.

Member of the CTN
Is a server that is a member of the CTN but does not currently have a role.

Time zone
Specifies the time zone for this system.

The Timer Server section also includes the following links to related tasks.

Manage System Time
Open the **Manage System Time** task for the selected DPM-enabled system.

Start Options

Use the Start Options details section to view partitions and groups of partitions that will be auto-started with the system. By default all group rows are expanded to show partitions in that group. Individual partitions and groups of partitions will be started in the order defined. The following list provides a description of each element on the Start Options details section:

The Start Options table toolbar

You can work with the table by using the table icons or **Actions** list from the table toolbar. Some actions are also available from a right click menu that applies only to the single row you right click (regardless of the table selections). If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar, right click menu, or both:

Export

Export as HTML
Downloads table data into a Hypertext Markup Language (HTML) file. This action is only available when you are using a remote browser.

Export All to CSV
Downloads table data into a Comma Separated Values (CSV) file. You can then import the downloaded CSV file into most spreadsheet applications. This action is only available when you are using a remote browser.

Print

Print All
Prints all rows in the table. This action is only available when you are using a remote browser.

Print Selected
Prints selected rows in the table. This action is only available when you are using a remote browser.

Print Preview
Displays a printable version of all rows in the table. This action is only available when you are using a remote browser.

Expand All
Expands all partitions groups in the Start Options table.

Collapse All
Collapses all partition groups in the Start Options table.

Columns in the Start Options table

The Processors table contains the following columns in the default display.

Name
Displays the name of a partition or a partition groups that will be auto-started with the system.

Post-Start Delay
Indicates the amount of time (in seconds) for the console to wait after starting one partition and before starting the next partition, when starting multiple partitions. If a partition is a member of a group, the Post-Start Delay column for the partition in the group is blank.

Description
Displays the user-provided description, if any, of the partition or partition group.

System Information

Accessing the System Information task

The Support Element automatically keeps records of information about the internal code changes stored on it. The record-keeping begins when changes are retrieved from their source to the Support Element.

For each internal code change, the information identifies:

- Its engineering change (EC) number.
- The change level most recently retrieved.
- The highest retrieved internal code change level that can be installed and activated concurrently.
- The change level most recently installed.
- The change level most recently activated.
- The change level most recently accepted.
- The lowest installed change level that can be removed and activated concurrently.
- The lowest change level that can be activated after removing installed change levels.
- Additional details include the most recent date and time each task was performed.

The information may assist you with planning and managing internal code changes. For example, review the information to either:

- Determine whether the system is operating with your latest available levels of internal code changes.

- Determine which tasks you must perform next to make the system operate with your latest available levels of internal code changes.

You can use the Support Element of a system to display information about the internal code changes stored on it. It also lists the part number, engineering change (EC) number and state levels of each set of licensed internal code associated with the Support Element.

Licensed internal code controls many of the operations available on the Support Element. Internal code changes may provide new operations, or correct or improve existing operations.

The part number and EC number are assigned to a set of licensed internal code by product support. The numbers identify the licensed internal code and its purpose.

If a set of licensed internal code is modified, its EC number is supplemented with a state level. A state level distinguishes between different versions of the same set of licensed internal code.

To view internal code change information:

1. Open the **System Information** task.

   The System Information window displays. It displays internal code change information.
2. Select the internal code information you want and then click **EC Details...** to view the additional information about this internal code.
3. Click **Query Additional Actions...** to display information about further actions that may be needed.
4. Click **OK** when you have completed this task.

System Information

Use this window to display information about the system and its internal code changes.

Information about the system identifies its machine type, model number, and serial number.

Information about the internal code changes is a record of tasks performed on the changes in the internal code change process. Additional details about specific internal code changes can also be requested.

The information may assist you with planning and managing the internal code change process. For example, review the information to either:

- Determine whether the system is operating with your latest available levels of internal code changes.
- Determine which tasks you must perform next to make the system operate with the latest available levels of internal code changes.

Note: Service representatives will provide assistance applying and managing internal code changes.

Machine Information

EC number
Displays the Engineering Change (EC) number of the system where the internal code changes are applied.

Type
Displays the machine type of the system where the internal code changes are applied.

Version
Displays the version of the system where the internal code changes are applied.

LIC control level
Displays the Licensed Internal Code level of the system where the internal code changes are applied.

Model number
Displays the machine model number of the system where the internal code changes are applied.

Engineering Changes AROM
This label is displayed when the system is preloaded for disruptive activation of a new Engineering Changes (ECs) level.

Concurrent Engineering Changes AROM
This label is displayed when the system is preloaded for concurrent activation of a new Engineering Changes (ECs) level.

Serial number
Displays the machine serial number of the system where the internal code changes are applied.

Driver
Displays the driver level of the system where the internal code changes are applied.

Note: The Driver information only appears if you are using this task with a user ID definition that is based on the *Service Representative* task roles.

Bundle level
Displays the bundle level of the system where the internal code changes are applied.

Internal Code Change Information

For additional information about an internal code change, select an EC number, then click **EC Details...**.

EC Number
Displays the engineering change (EC) number of the internal code change.

Retrieved Level
Displays the internal code change level that was most recently copied to the Support Element of the system, making it available for installation.

Installable Concurrent
Displays the highest retrieved internal code change level that can be installed and activated concurrently. That is, you can install and activate all change levels retrieved for this system, from the current installed level up to and including the installable concurrent level, without disrupting the operating system activity of the system.

Activated Level
Displays the internal code change level that was most recently activated as a working part of the licensed internal code of the system.

Accepted Level
Displays the internal code change level that was most recently made a permanent working part of the licensed internal code of the system.

Description
Displays a brief description of the internal code change.

Additional functions are available from this window:

EC Details...
To display detailed information for the selected internal code change, click **EC Details...**.

Query Additional Actions...
To display information for additional actions that are pending, click **Query Additional Actions...**. The **System Information Query Additional Actions** window is displayed. If further actions are required, instructions are provided, otherwise **NO** appears. Click **OK** to close the window.

View LIC Alerts...
To display additional information for the licensed internal code changes that have been retrieved but not yet installed and activated, click **View LIC Alerts...**. The **Licensed Internal Code Activation Alert** window displays. If further action is required, the window displays a message; otherwise, a message indicating no alerts to display for internal code changes displays.

OK
To close this window, click **OK**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Retrieved Level

This field displays the internal code change level that was most recently copied to the Support Element of the system, making it available for installation.

Compare the number in this field with the number displayed for the **installed level** to determine whether your latest available change level has been installed:

- If the retrieved level is higher than the installed level, then the change level has been retrieved, but has not been installed.

  The system, when activated, will operate without your latest available level of the internal code change.
- If the retrieved level is equal to the installed level, then the change level has been retrieved and installed.

  The system, when activated, will operate with your latest available level of the internal code change.

Installable Concurrent

This field displays the highest retrieved internal code change level that can be installed and activated concurrently. That is, you can install and activate all change levels retrieved for a system, from the current installed level up to and including the installable concurrent level, without disrupting the operating system activity of the system.

Compare the number in this field with the number displayed for the **installed level** to determine whether one or more retrieved change levels can be installed and activated concurrently:

- If the installable concurrent level is blank, then none of the retrieved change levels from the current installed level up to and including the current retrieved level can be installed and activated concurrently.
- If the installable concurrent level is equal to the installed level, then all of the retrieved change levels that can be installed and activated concurrently are already installed.

  Note: Compare the installable concurrent level with the **activated level**. If they are equal, then the installed concurrent change levels are also already activated. Otherwise, you can use console tasks for changing internal code to activate concurrent internal code changes for the system.
- If the installable concurrent level is higher than the installed level, then all retrieved change levels from the current installed level up to and including the installable concurrent level can be installed and activated concurrently.

  Note: You can use console tasks for changing internal code to install and activate concurrent internal code changes for the system.

  For example, when:

  – The **Installed Level** is: 002.

  – And the **Installable Concurrent Level** is: 004.

  Then you can use console tasks for changing internal code to install change levels: 003 and 004, and then activate them without disrupting the operating system activity of the system.

Activated Level

This field displays the internal code change level that was most recently activated as a working part of the licensed internal code of a system.

Compare the number in this field with the number displayed for the **installed level** to determine whether a more recent change level has been installed:

- If the installed level is higher than the activated level, then a more recent change level has been installed, but has not been activated.

  The system is operating without your latest available level of the internal code change.
- If the installed level is equal to the activated level, then the change level has been installed and activated.

Note: Compare the installed level with the **retrieved level** to determine whether the system is operating with your latest available level of the internal code change.

If the retrieved change level is installed and activated, compare the number in this field with the number displayed for the **accepted level** to determine whether your latest available change level has been accepted:

- If the activated level is higher than the accepted level, then the change level has been activated, but has not been accepted.

  The system is operating with your latest available level of the internal code change, but it is not yet a permanent working part of the licensed internal code of the object.
- If the activated level is equal to the accepted level, then the change level has been activated and accepted.

  Your latest available level of the internal code change is a permanent working part of the licensed internal code of the system.

Accepted Level

This field displays the internal code change level that was most recently made a permanent working part of the licensed internal code of the system.

Compare the number in this field with the number displayed for the **activated level** to determine whether a more recent change level has been activated:

- If the activated level is higher than the accepted level, then a more recent change level is currently activated, but it is not yet a permanent working part of the licensed internal code of the system.
- If the accepted level is equal to the activated level, then the change level currently activated is a permanent working part of the licensed internal code of the system.

  Note: Check the **retrieved level** and **installed level** to determine whether the system is operating with your latest available level of the internal code change.

System Information

Use this task to display information about the system and its internal code changes.

Information about the system identifies its machine type, model number, and serial number.

Information about the internal code changes is a record of tasks performed on the changes in the internal code change process. Additional details about specific internal code changes can also be requested.

The information may assist you with planning and managing the internal code change process. For example, review the information to either:

- Determine whether the system is operating with your latest available levels of internal code changes.
- Determine which tasks you must perform next to make the system operate with the latest available levels of internal code changes.

Note: A service representative will provide assistance applying and managing internal code changes.

Machine Information

EC number
Displays the Engineering Change (EC) number of the system where the internal code changes are applied.

Type
Displays the machine type of the system where the internal code changes are applied.

Version
Displays the version of the system where the internal code changes are applied.

LIC control level
Displays the Licensed Internal Code level of the system where the internal code changes are applied.

Model number
Displays the machine model number of the system where the internal code changes are applied.

Engineering Changes AROM
This label is displayed when the system is preloaded for disruptive activation of a new Engineering Changes (ECs) level.

Concurrent Engineering Changes AROM
This label is displayed when the system is preloaded for concurrent activation of a new Engineering Changes (ECs) level.

Serial number
Displays the machine serial number of the system where the internal code changes are applied.

Driver
Displays the driver level of the system where the internal code changes are applied.

Note: The Driver information only appears if you are using this task with a user ID definition that is based on the *Service Representative* task roles.

Bundle level
Displays the bundle level of the system where the internal code changes are applied.

Note: This information is not available for IBM zEnterprise 196 and IBM zEnterprise 114 machines and earlier.

Internal Code Change Information

For additional information about an internal code change, select an EC number, then click **EC Details...**.

EC Number
Displays the engineering change (EC) number of the internal code change.

Retrieved Level
Displays the internal code change level that was most recently copied to the Support Element of the system, making it available for installation.

Installable Concurrent
Displays the highest retrieved internal code change level that can be installed and activated concurrently. That is, you can install and activate all change levels retrieved for this system, from the current installed level up to and including the installable concurrent level, without disrupting the operating system activity of the system.

Activated Level
Displays the internal code change level that was most recently activated as a working part of the licensed internal code of the system.

Accepted Level
Displays the internal code change level that was most recently made a permanent working part of the licensed internal code of the system.

Description
Displays a brief description of the internal code change.

Additional functions are available from this window:

EC Details...
To display detailed information for the selected internal code change, click **EC Details...**.

Query Additional Actions...
To display information for additional actions that are pending, click **Query Additional Actions...**. The **System Information Query Additional Actions** window is displayed. If further actions are required, instructions are provided, otherwise **NO** appears. Click **OK** to close the window.

View LIC Alerts...
To display additional information for the licensed internal code changes that have been retrieved but not yet installed and activated, click **View LIC Alerts...**. The **Licensed Internal Code Activation Alert**

window displays. If further action is required, the window displays a message; otherwise, a message indicating no alerts to display for internal code changes displays.

OK
To close this window, click **OK**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Retrieved Level

This field displays the internal code change level that was most recently copied to the Support Element of the system, making it available for installation.

Compare the number in this field with the number displayed for the **installed level** to determine whether your latest available change level has been installed:

- If the retrieved level is higher than the installed level, then the change level has been retrieved, but has not been installed.

  The system, when activated, will operate without your latest available level of the internal code change.
- If the retrieved level is equal to the installed level, then the change level has been retrieved and installed.

  The system, when activated, will operate with your latest available level of the internal code change.

Installable Concurrent

This field displays the highest retrieved internal code change level that can be installed and activated concurrently. That is, you can install and activate all change levels retrieved for a system, from the current installed level up to and including the installable concurrent level, without disrupting the operating system activity of the system.

Compare the number in this field with the number displayed for the **installed level** to determine whether one or more retrieved change levels can be installed and activated concurrently:

- If the installable concurrent level is blank, then none of the retrieved change levels from the current installed level up to and including the current retrieved level can be installed and activated concurrently.
- If the installable concurrent level is equal to the installed level, then all of the retrieved change levels that can be installed and activated concurrently are already installed.

  Note: Compare the installable concurrent level with the **activated level**. If they are equal, then the installed concurrent change levels are also already activated. Otherwise, you can use console tasks for changing internal code to activate concurrent internal code changes for the system.
- If the installable concurrent level is higher than the installed level, then all retrieved change levels from the current installed level up to and including the installable concurrent level can be installed and activated concurrently.

  Note: You can use console tasks for changing internal code to install and activate concurrent internal code changes for the system.

  For example, when:

  – The **Installed Level** is: 002.

  – And the **Installable Concurrent Level** is: 004.

  Then you can use console tasks for changing internal code to install change levels: 003 and 004, and then activate them without disrupting the operating system activity of the system.

Activated Level

This field displays the internal code change level that was most recently activated as a working part of the licensed internal code of a system.

Compare the number in this field with the number displayed for the **installed level** to determine whether a more recent change level has been installed:

- If the installed level is higher than the activated level, then a more recent change level has been installed, but has not been activated.

  The system is operating without your latest available level of the internal code change.
- If the installed level is equal to the activated level, then the change level has been installed and activated.

  Note: Compare the installed level with the **retrieved level** to determine whether the object the system is operating with your latest available level of the internal code change.

If the retrieved change level is installed and activated, compare the number in this field with the number displayed for the **accepted level** to determine whether your latest available change level has been accepted:

- If the activated level is higher than the accepted level, then the change level has been activated, but has not been accepted.

  The systemis operating with your latest available level of the internal code change, but it is not yet a permanent working part of the licensed internal code of the system.
- If the activated level is equal to the accepted level, then the change level has been activated and accepted.

  Your latest available level of the internal code change is a permanent working part of the licensed internal code of the system.

Accepted Level

This field displays the internal code change level that was most recently made a permanent working part of the licensed internal code of the system.

Compare the number in this field with the number displayed for the **activated level** to determine whether a more recent change level has been activated:

- If the activated level is higher than the accepted level, then a more recent change level is currently activated, but it is not yet a permanent working part of the licensed internal code of the system.
- If the accepted level is equal to the activated level, then the change level currently activated is a permanent working part of the licensed internal code of the system.

  Note: Check the **retrieved level** and **installed level** to determine whether the system is operating with your latest available level of the internal code change.

Internal Code Change Details

This window displays details for an internal code change.

Attention: A service representative will provide new internal code changes and manage their initial use.

For internal code changes already retrieved, you should manage these changes only under the supervision of a service representative or with the assistance of the support system.

Selected Internal Code Change Item

Part number
Displays the part number of the internal code change.

Engineering change number
Displays the engineering change (EC) number of the internal code change.

Engineering change type
Identifies the type of internal code affected by the internal code change.

Base ECs
Indicates the internal code change affects the base internal code of the system.

National language EC
Indicates the internal code change affects the internal code for a specific national language.

Other optional EC
Indicates the internal code change affects internal code other than base or national language internal code.

Engineering change description
Displays a brief description of the internal code change.

Internal Code Change State Details

Type
Identifies the internal code change states of an internal code change.

Level
Displays the change level of the selected internal code change in the state.

Date
Displays the date the change level was put in the state.

Time
Displays the time the change level was put in the state.

Additional functions are available from this window:

OK
To close this window and return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

System Information Error

An error occurred when attempting to retrieve the system information for the objects listed below.

Use this window to view system information retrieval error details.

Select an object, click **Error Details...** to view the cause for this error.

OK
To close this window, click **OK**.

Error Details...
To view the cause for the selected error, click **Error Details...**.

Help
To display help for the current window, click **Help**.

System Input/Output Configuration Analyzer

Accessing the System Input/Output Configuration Analyzer task

Use this task to view and analyze your current I/O configuration. The data can be viewed in several different arrangements giving emphasis to one item. You may filter the data and it will be applied to all applicable views.

To view and analyze your current I/O configuration:

1. The central processor complex (CPC) must be power-on reset.
2. Locate the **CPC** to work with.
3. Open the **System Input/Output Configuration Analyzer** task.

   The System Input/Output Configuration Analyzer window displays.

4. Select a choice from the following menu bar:
   - **File** to save data to a USB flash memory drive, refresh the display window, or exit the current window.
   - **View** to display different views for the current I/O configuration data.
   - **Filter** to filter out or to display specific information for the current I/O configuration.
   - **Sort** to sort the current view using parameters specified.
5. Select **Exit** from the **File** menu bar to exit the task.

System Input/Output Configuration Analyzer

Use **System Input/Output Configuration Analyzer** to analyze and help manage your current I/O configuration on the support element.

Note: Any dynamic changes have to be saved and made active on the Support Element to display in the tool.

The data can be viewed in several different arrangements giving emphasis to one item.

- You may filter the data and it will be applied to all applicable views.
- You may sort the data for the view you are currently observing. However, the results when sorting on the PCHID control unit or PCHID partition views will be grouped together.

File

To perform an action to save displayed data for the current I/O configuration, refresh, or exit the window, select **File** from the menu bar. The following choices are available from the **File** drop-down menu:

Save Data to USB Flash Memory Drive

To save displayed data for the current I/O configuration to a USB flash memory drive, click **Save Data to USB Flash Memory Drive**.

Note: This option is only available if you are accessing the console locally.

Plug the USB flash memory drive into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message is displayed indicating the drive was not added and that you should remove the device and try again.

Save Data via FTP

To save displayed data for the current I/O configuration to a secure FTP location, click **Save Data via FTP**.

Refresh

To update the display window with the current I/O configuration data, click **Refresh**.

Exit

To end this task and return to the workplace, click **Exit**.

View

To display different views for the current I/O configuration data, select **View** from the menu bar. The following choices are available from the **View** drop-down menu:

PCHID Control Unit

Displays the current I/O configuration data by the PCHID control unit.

PCHID Partition

Displays the current I/O configuration data by the PCHID partition.

Control Unit

Displays the current I/O configuration data by the control unit.

Link Load

Displays the current I/O configuration data by the link load.

Node ID
Displays the current I/O configuration data by the node ID.

Filter
To filter out or to display specific information for the current I/O configuration, select **Filter**. The data entered is applied to all the views that contain the data and the information is displayed. From the menu, select the data that you want to be filtered. Some of the filter options may include:

PCHID
Allows you to enter the PCHID to filter on.

CSS.CHPID
Allows you to enter the CSS.CHPID to filter on.

Switch
Allows you to enter the switch to filter on.

Partition
Allows you to enter the partition to filter on.

Control Unit
Allows you to enter the control unit to filter on.

Show All
Allows you to display all the current I/O configuration data.

Sort
To sort the current view, select **Sort**. The data is sorted using the parameters specified and then the view is displayed. Only the current view is sorted with the exception of PCHID control unit and PCHID partition views. These views are tightly coupled.

Help
To display help for the current window, click **Help**.

System Input/Output Configuration Analyzer

Use this window to export displayed data for the current I/O configuration to a specified FTP destination. Use the **Protocol** field to select a secure network protocol for transferring files to the specified FTP destination.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

Additional functions on this window include:

Export
To export the displayed current I/O configuration data to an FTP destination, click **Export**.

Cancel
To close the window without saving your changes, click **Cancel.**

Help
To display help for the current window, click **Help**.

System Input/Output Configuration Analyzer - Filter

Use this window to enter specific data on how you want the data to be displayed (for example, if filtering PCHIDs and you entered 0120 then all data related to PCHID 0120 will be displayed). The data entered is applied to all the views that contain the data and the information is displayed.

OK
To perform the filter action you entered, click **OK**.

Cancel
To close the current window, click **Cancel**.

Help
To display help for the current window, click **Help**.

System Input/Output Configuration Analyzer - Sort

Use this window to enter specific data on how you want the current I/O configuration to sort the displayed information. If you want to sort the current window columns in ascending order, you must indicate it on the window.

OK
To perform the sort action you entered, click **OK**.

Cancel
To close the current window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Task Information

Object Selection

Use this window to select the object that the task will be performed on. This task can only be performed on a **single** object. Select an object from the Object Name list and click **OK**.

Object Name
This list displays the objects that may be targeted for the selected task.

Note: Only a single target object may be chosen at one time. Select an entry in the list to view the profile that will be used for that object.

OK
To perform the task on the object you chose, click **OK**.

Cancel
To end the task and exit the window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Secondary Object Notification for Disruptive Task

One or more of the objects to be targeted for the selected task have associated secondary objects that will also be affected by this task. The selected task is considered to be disruptive and will also cause disruption to the associated secondary objects. Use this window to review the list of secondary objects that will also be affected before continuing this task.

Service Status
This list displays the secondary objects that will be affected by the task as well as their current operating status.

Yes
To continue with the task, click **Yes**, understanding that the secondary objects listed will also be affected.

No
To end the task, click **No**, without disrupting the secondary objects.

Help
To display help for the current window, click **Help**.

Single Task Confirmation

Use this window to review the displayed objects before proceeding with the task.

Object Names
This list displays the objects that are to be targeted for the selected task.

Yes
To perform the task on the objects displayed in the list, click **Yes**.

No
To end the task and exit the window without saving any changes, click **No**.

Help
To display help for the current window, click **Help**.

Invalid Target Object List

This window appears when one or more of the targeted objects for a selected task have a status that would cause the task to fail. Use this window to view the list of objects targeted for the selected task and the reason the targeted objects can or cannot be used to perform the selected task.

Object Status
This list displays the object names and the reason why the object can or cannot perform the selected task. Review the object list to determine which objects are currently not valid for the task.

Yes

To continue the task with only the valid objects as targets, click **Yes**.

No

To end the task and exit the window, click **No**.

Help
To display help for the current window, click **Help**.

Multiple Task Confirmation

Use this window to review the displayed objects and confirmation text for each object before proceeding with the task.

Object Status
This list displays the objects that are to be targeted for the selected task.

Note: Select an entry in the list to view the profile that will be used for that object.

Yes
To perform the task on the objects displayed in the list, click **Yes**.

No
To end the task and exit the window without saving any changes, click **No**.

Help
To display help for the current window, click **Help**.

Task Progress

Targeted Progress

This window displays the estimated duration and elapsed time of an active task. The name of the task in progress is displayed in the window title.

This window is also for a task that has multiple targets. The table displays one line for each of the targets of the task. Each line includes the name and the task status of the objects on which the task is performed. These lines are updated one at a time as a task finishes its processing for each of the targets.

Estimated function duration time
This displays the estimated amount of time necessary to complete the task.

Note: The function duration time when deactivating an object may not match the elapsed time because the operating system installed on the object may respond differently to the shutdown request.

Elapsed time
This displays the actual amount of time that has passed as the task progresses.

OK
To close the window when the task completes, click **OK**.

Details...
To display additional information about the selected object, click **Details...**.

Force
To override the normal processing shutdown of the selected object without waiting for the operating system to respond, click **Force**.

Cancel
To cancel running the task, click **Cancel**. This is not available for all tasks. If **Cancel** is available and you click it, it becomes disabled while the task tries to end. **Cancel** does not close the window.

Help
To display help for the current window, click **Help**.

Force termination

Use this window to view object(s) that you are requesting a force termination.

Object Name
Displays the name of the object(s) to force a termination.

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Select All/Deselect All
You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block. Click **Select All** or **Deselect All** to select or deselect all objects in the table.

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want.

Clear All Filters
Click **Clear All Filters** to return to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions are available from this window:

OK
To continue with the force termination of the listed objects(s), click **OK**.

Cancel
To close the window without forcing a termination on the listed object(s), click **Cancel**.

Help
To display help for the current window, click **Help**.

Non-Targeted Progress

This window displays the estimated duration and elapsed time of an active task. The name of the task in progress is displayed in the window title.

This window is for a task that has a single target. The table displays progress information for the task.

Estimated function duration time
This displays the estimated amount of time necessary to complete the task.

Elapsed time
Displays the actual amount of time that has passed as the task progresses.

Progress table
This table displays the status of the task for the object. The status is a brief message indicating the progress of the task.

OK
To close the window when the task completes, click **OK**.

Details...
To display additional information about the object, click **Details...**.

Cancel
To cancel running the task, click **Cancel**. This is not available for all tasks. If **Cancel** is available and you click it, it becomes disabled while the task tries to end. **Cancel** does not close the window.

Help
To display help for the current window, click **Help**.

Toggle Lock

Accessing the Toggle Lock task

This task allows you to set a disruptive task lockout for the selected object.

Note: This task cannot be used on IBM Dynamic Partition Manager (DPM) objects.

To lockout an object:

1. Select the **Toggle Lock** task from the Tasks Index. The Target Object Selection window is displayed.
2. Choose one or more objects, then click **OK**. The object or objects selected displays a lock icon. This indicates that the object is locked and a disruptive task cannot be performed. If you want to remove the lock, select the **Toggle Lock** task again.

   Note: You can also select the object first and then click **Toggle Lock** from the Tasks area of the window.

For more information on Disruptive tasks and locking an object, go to the Help Table of Contents and select **Introduction** > **Disruptive tasks** > **Locking an object**.

Transmit Service Data

Accessing the Transmit Service Data task

Service data is a set of system information, such as program and event traces and storage dumps, collected by the support element of the system. Service data assists the service representative in servicing the problem.

Sending service data is necessary only when service data is requested, usually through either your service representative or support system. Typically, service data is requested after a problem is reported if analyzing the service data is necessary to determine the cause of the problem.

You can send service data either by copying it to a removable media device for delivery, by transmitting it through a remote connection to the support system, or by transmitting data to an FTP server.

Notes:

- Although the same service data is sent through each destination, the most direct destination is the support system. You can use the support system as a destination only by customizing, in advance, the system's remote service settings to *enable* remote service. See the **Remote Service** task for instructions for enabling remote service.
- If you are using a USB flash memory drive, plug it into the console and then wait for the console to beep three times. This indicates that the device is ready and can be accessed. If it does not been three times, unplug the device and try again.

To send service data to the support system:

1. Open the **Transmit Service Data** task.
2. Use the Transmit Service Data window, as directed by your service representative or support system, to select the service data requested.
3. Select the data you want to send and the destination for the data. You can also enter the related problem management number if it is known.
4. Click **Send** to transmit the selected data or **Cancel** to end the task without sending any data.

Transmit Service Data

Use this window to select the types of service data and how it is to be sent.

Service data is a set of program and event traces and storage dumps. The data in the traces and the contents of storage assists in servicing the system.

Use this window only when directed by your service representative or support system. Select the service data categories requested. Service data in selected categories is collected in a file or group of files for transmission.

Before you can send information to the support system, *call-home server* and *remote service* must be enabled.

Note: Some service data categories may not be available for selection. Such categories appear grayed. This indicates that no data is available for that category.

Service Categories:

"Service Data Destination" on page 867
Use this section to specify how your service data is sent.

Note: The removable media selection is the only destination allowed on the alternate SE.

"Service Data Selections" on page 868
Use the displayed categories in this section to select the types of service data to send.

Note: This option is not supported on the alternate Support Element.

"Remote Support Problem Number" on page 868
If provided, specify the case number.

Note: This option is not supported on the alternate Support Element.

"Virtual Support Repository Files" on page 869
Use this section to transmit a data service file or a group of data service files to the support system.

"IOCDS Files" on page 869
Use this section to send selected Support Element IOCDS files to the support system.

Note: This option is not supported on the alternate Support Element.

Additional functions are available from this window:

Send
To send service data to the selected destination, click **Send**. The Select Media Device window is displayed. From this window you can choose the media you want to send the data to. You can click **OK** to continue with the task, click **Refresh** to re-display your media selections, or click **Cancel** to return to the previous window.

Cancel
To exit this task without making any selections, click **Cancel**.

Reset
To clear current selections, click **Reset**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Service Data Destination

Use this section to specify how your service data is sent to the support system.

The following options are available:

Support System
To use the Remote Support Facility (RSF) to transmit the service data to the support system, select **Support System**.

Removable media
To copy the service data to a removable media (USB flash memory drive), select **Removable media**.

Notes:

- When you use a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.
- This option is not available if the console is running remotely.

FTP Server
To transfer data using an FTP server, select **FTP Server**.

Service Data Send to FTP Server

Use this window to configure FTP settings when you use an external server to transmit your files to the specified directory.

Host name
Specify the host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the **Manage SSH Keys** task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved. This is a required field.

Transmit
To submit this information to the specified directory, click **Transmit**.

Cancel
To close the window without providing information, click **Cancel**.

Help
To display help for the current window, click **Help**.

Service Data Selections

Use the displayed categories in this section to select the types of service data to send to the support system.

Select one or more service data categories as requested. Service data in selected categories is collected in a file or group of files for transmission to the support system.

Remote Support Problem Number

The remote support problem number is provided by a service representative.

The remote support problem number is associated with the transmitted data with an open case for this system. If the data being sent is not problem-oriented or a case number has not been issued to this system, then this field is optional.

Notes:

- The case number cannot be validated, however if an invalid case number is given, the transmitted data is still accepted.
- This option is not available on the alternate Support Element.

Authorized users can view a system's open cases on the IBM Support website: https://www.ibm.com/mysupport. For more details on IBM support, see: https://www.ibm.com/support/pages/note/733923.

Virtual Support Repository Files

Use this window to transmit a data service file or a group of data service files to the support system.

Note: This field is displayed only during a service call.

Enter the file name or a global file name (for example, **/console/data/driver.name** or **/console/data/driver.***), and then click **Send**.

List of restrictions on the file name:

- Only the console's hard drives are valid.
- Standard wild cards (* and ?) apply.
- Specifying an entire directory or subdirectory is not allowed.

FFDC Manager Files

Use this window to transmit a data service file or a group of data service files to the support system.

To open the **FFDC Manager Files** window, click **Select Files**. Once the window displays, select the file or files to transmit and then click **OK**. To exit the window without saving any file selections, click **Cancel**.

If you selected **OK**, then the **Selected resource count displays** the total number of files you selected on the FFDC Manager Files window.

Note: This field is only displayed during a service call.

IOCDS Files

Use this window to send selected Input/Output Configuration Data Set (IOCDS) files to the support system.

To open the **Select IOCDS files for transmission** window, click **Select Files**. Once the window displays, select the file or files to transmit and then click **OK**. To exit the window without saving any file selections, click **Cancel**.

Note: This option is not available on the alternate Support Element.

Transmit Vital Product Data (SE)

Accessing the Transmit Vital Product Data task

This task provides a window for you to collect Vital Product Data (VPD) from the Support Element and to either transmit the data to the support system or to store the information on USB flash memory drive or Support Element hard disk.

To send vital product data to the Support Element:

1. Open the **Transmit Vital Product Data** task. The Transmit Vital Product Data window is displayed.
2. Select the destination to which you want to transmit:
   - Support system
   - USB flash memory drive
   - Support Element hard disk

   and then click **OK** to proceed.

Transmit Vital Product Data

Use this window to select a method for sending the VPD to the support system. Confirm or cancel your request to send Vital Product Data (VPD) to the support system, but only for machines with complete VPD.

Vital Product Data Destination
Select the vital product data destination, then click **OK**.

Support system
To transmit vital product data to support system, select **Support system**.

The console must be equipped and enabled for using the Remote Support Facility (RSF) to use this destination.

The Support Element must be equipped and enabled for using the Remote Service Facility (RSF) to use this destination.

USB flash memory drive
To copy vital product data to a USB flash memory drive, select **USB flash memory drive**.

Then insert a USB flash memory drive into a USB port, and click **OK**.

Note: If you are using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

Support Element
To copy vital product data to the hard disk, select **Support Element hard disk**.

FTP server
To copy vital product data to an FTP server, select **FTP server**. Use the **Protocol** field to specify a secure network protocol for transferring files to the specified FTP destination. Use the **File path** field to type the file path directory where the files are to be saved or read.

Host name
Specify the FTP host name address or destination. This is a required field.

User name
Specify the user name for the target FTP destination. This is a required field.

Password
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol
Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)

  If you need to import an FTPS server certificate, use the **Certificate Management** task. From the **Advanced** drop-down select **Manage Trusted Signing Certificate**. The Manage Trusted Signing Certificate window is displayed. From the **Import** drop-down, select **From Remote Server**. The Import Remote Certificate window is displayed. Provide the IP/Host address and port number, then click **OK** to confirm. The Confirm Import window is displayed, then click **Yes** after you verified the certificate information.
- **SFTP** (SSH File Transfer Protocol)

  If you need to import SSH server keys, use the Manage SSH Keys task. Provide the SFTP server ID in the **Address** input area, then click **Add**.

File path
Specify the FTP server directory where files are to be saved to or read from.

OK
To transmit vital product data to the support system based on the selections that you chose, click **OK**. If you selected media as the destination, the **Select Media Device** window is displayed. From this window you can choose the media you want to send the data to. You can click **OK** to continue with

the task, click **Refresh** to redisplay your media selections, or click **Cancel** to return to the previous window.

Cancel
To close this window without transmitting vital product data to the support system, click **Cancel**.

Help
To display help for the current window, click **Help**.

Update HOM and VPD

Accessing the Update HOM and VPD task

Use this task to update the hardware configuration and vital product data to reflect the current LICCC data.

To update HOM and VPD:

1. Open the **Update HOM and VPD** task.

   The Update Hardware Configuration and VPD window displays.
2. Click **OK** to update the hardware configuration and vital product data or click **Cancel** to leave this task without making any updates.
3. If you click **OK**, a message appears indicating the update was successful. Click **OK** to close the message window.

Update I/O World Wide Port Number

Accessing the Update I/O World Wide Port Number task

To update the I/O world wide port number:

1. Locate and open the **Update I/O World Wide Port Number** task.
2. Enter the new I/O world wide port number for the upgraded system.
3. Click **OK** to update.

Update I/O World Wide Port Number

Use this window to update the I/O world wide port number of the Vital Product Data (VPD) when upgrading your system.

You can find more detailed help on the following elements of this window:

OK
To update the new I/O world wide port number, click **OK**.

Cancel
To close the window without saving changes and return to the previous window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Update PCI Adapter Internal Code

Accessing Update PCI Adapter Internal Code task

To update PCI adapter internal code:

1. Locate and open the **Update PCI Adapter Internal Code** task.

   The Update PCI Adapter Internal Code window displays.

Update PCI Adapter Internal Code

Use this window to view and update the PCI adapters which have pending internal code updates for the selected PCHIDs.

You can work with the table by using the table icons or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

PCHID
Indicates the PCHID that is assigned to the PCHID adapter

State
Indicates the current state of the PCHID

Status
Indicates the current status for the selected PCHID

Type
Indicates the PCI adapter type for the selected PCHID

Number of Online IDs
Indicates the number of online PCI adapter IDs. Select the hyperlink to display the PCI adapter IDs associated the PCHID

Adapter Changes Pending Install and Activate
Indicates there are staged MCL updates which causes the Update Pending conditions once an Install/Activate is performed for the selected PCHID. It is recommended to use the **Change Internal Code** task prior to updating the selected PCHID.

Note: This column displays for SERVICE mode only.

Pending Update
Indicates a PCI adapter internal code update is pending for the selected PCHID.

The icons perform the following functions in the PCHID definition table:

Select All/Deselect All
You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block. Click **Select All** or **Deselect All** to select or deselect all objects in the table.

Show Filter Row
Displays a row under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. You can filter tables to show only those entries most important to you. You can toggle the filtered view on and off by selecting the filter that you want.

Clear All Filters
Click **Clear All Filters** to return to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

Edit Sort
Performs multi column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, to perform single column sorting, click the **^** in the column header, to change from ascending to descending order.

Clear All Sorts
Click **Clear All Sorts** to return to the default ordering.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Additional functions on this window include:

Update Adapter Firmware
To update the firmware internal code on the selected PCHID(s), select **Update Adapter Firmware**.

Close
To close this window and exit this task, click **Close**.

Help
To display help for the current window, click **Help**.

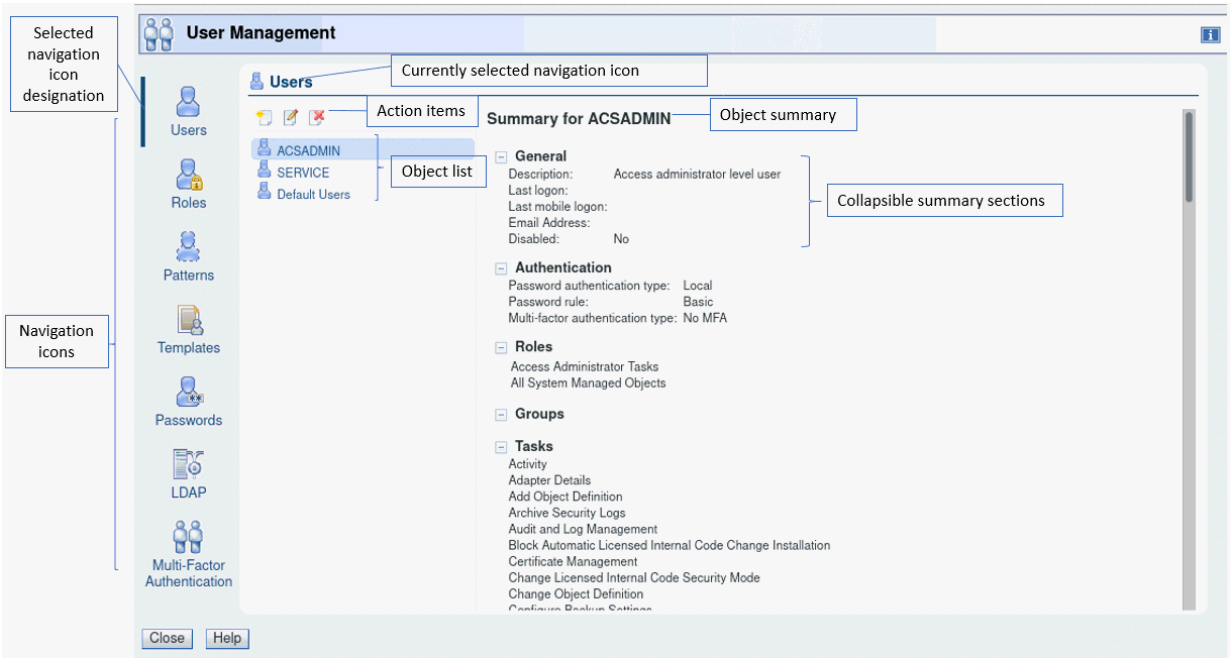
User Management

Accessing the User Management task

This task is used by an access administrator or a user that is assigned Access Administrator Tasks role to manage users, roles, user patterns, user templates, password rules, LDAP server definitions, and multi-factor authentication for your system users that log on to the console. This task can also be used when no administrator role is provided as view only for their own user information. The user can change their own password and set a default group.

To manage user access and permissions to the console:

1. Open the **User Management** task in access administrator role. The **User Management** dashboard is displayed.



2. Select the icon for the area of user management you want to customize. Users is the first icon in the navigation pane and is the default selection when the User Management dashboard is opened.
3. Select a currently defined object from the object list to view the current values in the object summary area.
4. Select the icons above the objects list to perform the following actions:

   New
   To create a new object

   Details
   To view or modify existing properties for the selected object

   Delete
   To delete the selected object

User Management

This task gives the access administrator a common area to view and manage users, roles, user patterns, user templates, password rules, and LDAP server definitions for your system. The navigation icons on the dashboard are listed in the order of highest usage and not the sequence an administrator would use to initially set up access to the console. See "Getting Started" on page 876 for some scenarios to assist an administrator with first time usage of the **User Management** dashboard. See "Default Permissions" on page 888 for the list of permissions that are granted to every user by default and therefore not shown on the **User Management** dashboard.

To use the User Management dashboard:

1. Select the icon for the area of user management you want to customize. Users is the first icon in the navigation pane and is the default selection when the User Management dashboard is opened.

   Note: Only icons permitted for the current user display (For example, the **Roles** icon is shown to users who have permission to the **Manage User Roles** task.) See the navigation icon description for the permissions that correspond to the icons.
2. Select a currently defined object from the object list to view the current values in the object summary area.
3. Select the icons above the objects list to perform the following actions:

   New
   To create a new object

   Details
   To view or modify existing properties for the selected object

   Delete
   To delete the selected object

The navigation icons are as follows:


Users

A *user* object defines the user's authentication, roles which determine access permissions, and a default group to which any objects created by the user will be added. Select "Users" on page 889 to create a new user or modify user properties. Permission to the **Manage Users** task is required for the capability of managing users other than the current user.


Attention: The use of default passwords are no longer allowed. The first time a default user ID logs on to the console, the default password must be changed. A prompt is displayed requiring the password change. This is initiated in this task by SERVICE or a user that is assigned a role with Manage Users task permission.


Roles

A *role* defines permissions to tasks, type of objects or specific objects, groups, and task lists. Select "Roles" on page 897 to create a new role or modify role properties. Permission to the **Manage User Roles** task is required for the icon and corresponding dashboard view to be available.


User Patterns

A *user pattern* is used to automatically create users on this system based on successful authentication of user IDs that conform to a defined string pattern. The user pattern requires a template definition to specify the user capabilities. Select "User Patterns" on page 906 to create a new user pattern or modify user pattern properties. Permission to the **Manage User Patterns** task is required for the icon and corresponding dashboard view to be available.

User Templates

A *user template* defines the settings and permissions for users authenticated with a user pattern. The template requires an LDAP server definition. Select "User Templates" on page 915 to create a new user template or modify user template properties. Permission to the **Manage User Templates** task is required for the icon and corresponding dashboard view to be available.

Password Rules

A *password rule* defines a set of rules to be used when creating a user password. Select "Password Rules" on page 921 to create a new password rule or modify password rule properties. Permission to the **Manage Password Rules** task is required for the icon and corresponding dashboard view to be available.

LDAP Server Definitions

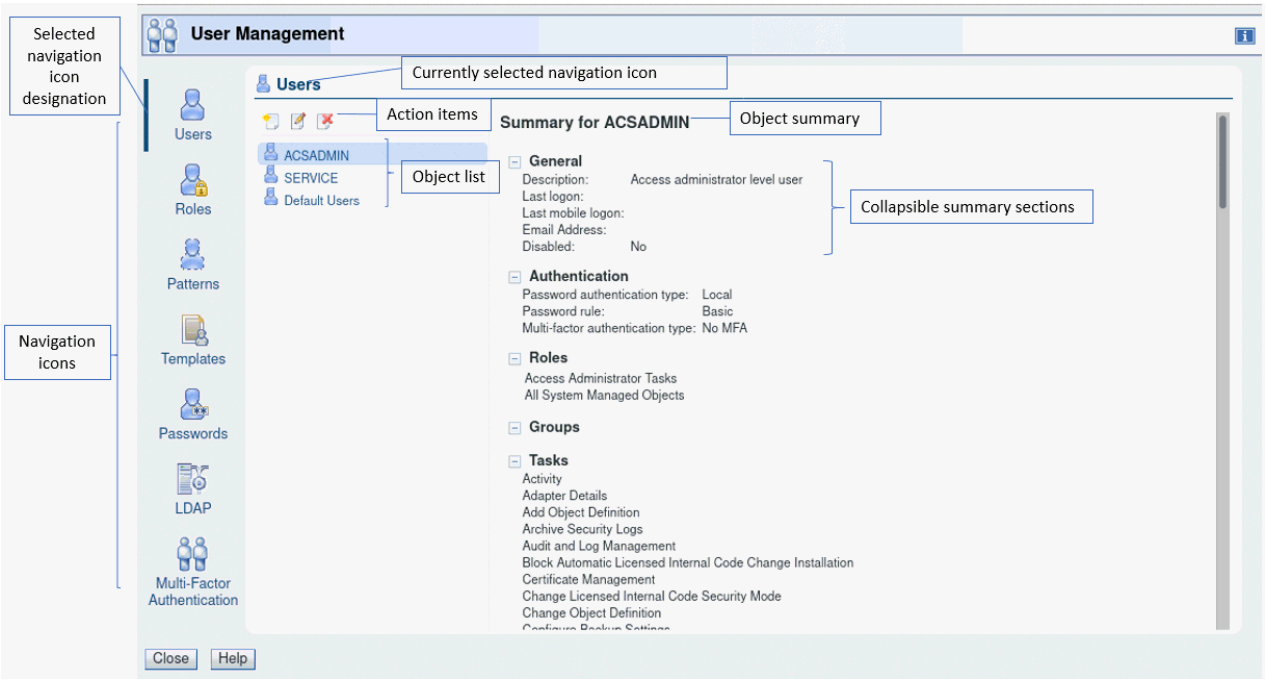
An *LDAP server definition* specifies host connection and directory entry location information to be used for authentication. Select "LDAP Server Definitions" on page 927 to create a new LDAP server definition or modify LDAP server definitions. Permission to the **Manage LDAP Server Definitions** task is required for the icon and corresponding dashboard view to be available.

Multi-Factor Authentication

A *multi-factor authentication* requires additional security tokens to verify the identity of a user when logging on to the console. Select "Multi-Factor Authentication" on page 932 to enable multi-factor authentication for users and user templates. Permission to the **Manage Multi-factor Authentication** task is required for the icon and corresponding dashboard view to be available.

Note: Each of the views for the User Management dashboard is only displayed if the current user has access to their corresponding task.

The user management interface is comprised of several major components: the navigation icon area, the object list, and the object summary.



Navigation icon area
The navigation icon area is located in the left portion of the window and provides a common area for an administrator to work with all aspects of user access to the console. You can hover over the icons to display the name of the icons.

Object list
The object list contains a list of the currently defined objects for the selected navigation icon.

Object summary
The object summary displays the current values for the selected item in the object list.

Getting Started

The **User Management** dashboard provides a common area for an administrator to work with all aspects of user access to the console. This section gives some common scenarios and the detailed steps for using the dashboard to accomplish a specific goal. The scenarios touch on each of the navigation areas: Users, Roles, User Patterns, User Templates, Password Rules, LDAP Server Definitions, and Multi-factor Authentication. Any reference to a page in the step-by-step instructions refers to the page listed in the left navigation (which might not match the page title).

The list of scenarios for getting started with the **User Management** dashboard are as follows. Click the links, in any order, to get the step-by-step details to accomplish the goal.

User default changes from Version 2.13.1 to Version 2.14.0

The table below lists the default changes from Version 2.13.1 to Version 2.14.0 for increased security and ease of use.

Table 4. User default changes from Version 2.13.1 to Version 2.14.0

Setting	**Previous Default (Version 2.13.1)**	**New Default (Version 2.14.0)**
New User		
Email address	Not available	Provide address to enable; requires Simple Mail Transfer Protocol (SMTP) setup in **Monitor System Events** task
User Pattern		
User setting retention time	Disabled, now suggesting 1 when enabled	90 days
Multi-factor Authentication		
Multi-factor Authentication	Not available	Select users and templates to enable
Reset shared secret keys	Not available	Select users and templates to reset

User default changes from Version 2.12.1 to Version 2.13.0

The table below lists the default changes from Version 2.12.1 to Version 2.13.0 for increased security and ease of use.

Table 5. User default changes from Version 2.12.1 to Version 2.13.0

Setting	**Previous Default (Version 2.12.1)**	**New Default (Version 2.13.0)**
New User		
Description	Required	Not required

Table 5. User default changes from Version 2.12.1 to Version 2.13.0 (continued)

Setting	Previous Default (Version 2.12.1)	New Default (Version 2.13.0)
Password rule	Basic	Standard
Force user to change password	Not checked	Checked
Managed objects/roles	Required to select 1 or more of each	Not required
Session timeout	Disabled, indicated by 0	Disabled, now suggesting 300 when enabled
Idle timeout	Disabled, indicated by 0	Disabled, now suggesting 20 when enabled
Delay login after failed attempts	Disabled	Enabled
Number of failed attempts before disable delay	0	3
Delay (minutes) (for login delay after failed attempts)	0	1
Minimum time between password changes	Disabled, indicated by 0	Disabled, now suggesting 1440 when enabled
User Pattern		
Description	Required	Not required
User setting retention time	Blank, user must specify a value	Disabled, now suggesting 1 when enabled
User Templates		
Description	Required	Not required
Managed objects/roles	Required to select 1 or more of each	Not required
Session timeout	Disabled, indicated by 0	Disabled, now suggesting 300 when enabled
Idle timeout	Disabled, indicated by 0	Disabled, now suggesting 20 when enabled
Delay login after failed attempts	Disabled	Enabled
Number of failed attempts before disable delay	0	3
Delay (minutes) (for login delay after failed attempts)	0	1
Password Rule		
Case sensitive	No	Yes
LDAP Server		
Connection port	Blank	389

Table 5. User default changes from Version 2.12.1 to Version 2.13.0 (continued)		
Setting	**Previous Default (Version 2.12.1)**	**New Default (Version 2.13.0)**
Use SSL connection	No change to connection port when toggled	Changes connection port from 389 to 636 when toggled

Create a new user

The goal of this scenario is to create a new user for John. John requires the system programmer level authority and access to all system resources (all objects of all types).

Steps to create a new user:

1. From the **User Management** dashboard, select the **Users** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New User** wizard is started.
3. On the Welcome page of the **New User** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, select **New**. In the User Details section enter *John* in the Name field. Optionally, enter meaningful text in the Description field to describe your user, and enter a valid email address in the Email address field. Then click **Next**.
5. On the Authentication page, keep the default selection **SE password authentication**. Leave the Password rule as the default *Standard*. Enter *johnpw* as the password in the Password and Confirm password fields, then click **Force user to change the password at next logon**, and then click **Next**.
6. On the Roles page, select the roles *Defined System Managed Objects* and *System Programmer Tasks*. You can also select the check box for role *All Resources* to give John access to all objects of all types. Optionally, you can clear the check box on the row for role *Defined System Managed Objects*, since these permissions are contained in the *All Resources* role. When complete, click **Next**.

   Note: You can click on the links for the roles to open **Role Details** for that role. If desired, you can make modification to user-defined roles from **Role Details**.
7. Review the details on the Summary page, then click **Finish**. The user John is created.
8. On the dashboard, user *John* is added to the Users list and is the current selected user. View the *Summary for John* to see the Roles, Groups, Tasks, Object Types, and Objects that John is granted permission.

John is now able to logon to the console with user ID *john* and password *johnpw*. John is required to change the password the first time he logs on.

Create a new user based on a system default user

The goal of this scenario is to create a new user for John based on the ACSADMIN default user. John requires the Access Administrator level authority and access to all system resources (all objects of all types).

Steps to create a new user based on a system default user:

1. From the **User Management** dashboard, select the **Users** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New User** wizard is started.
3. On the Welcome page of the **New User** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, select **New based on**. Click the drop-down list for the based on user and select *ACSADMIN*. In the User Details section enter *John* in the Name field.

Optionally, enter meaningful text in the Description field to describe your user, and enter a valid email address in the Email address field. Then click **Next**.

5. On the Authentication page, keep the default selection **SE password authentication**. Leave the Password rule as the default *Standard*. Enter *johnpw* as the password in the Password and Confirm password fields, then click **Force user to change the password at next logon**, and then click **Next**.
6. On the Roles page, the roles *Access Administrator Tasks*, and *All System Managed Objects* are preselected from the ACSADMIN user. Select the check box for role *All Resources* to give John access to all objects of all types. When complete, click **Next**.

   Note: You can click on the links for the roles to open **Role Details** for that role. If desired, you can make modification to user-defined roles from **Role Details**.
7. Review the details on the Summary page, then click **Finish**. The user John is created.
8. On the dashboard, user *John* is added to the Users list and is the current selected user. View the *Summary for John* to see the Roles, Groups, Tasks, Object Types, and Objects that John is granted permission.

John is now able to logon to the console with user ID *john* and password *johnpw*. John is required to change the password the first time he logs on.

Create a single customized role containing all desired task and object permissions

The **User Management** task provides the capability to include all desired permissions for tasks, objects, groups, and task lists in a single role. For administrators who are familiar with the **Customize User Controls** task in HMC version 2.12.1, **Customize User Controls** required separate roles to specify permissions for tasks, and separate roles for each object type. This scenario creates a single role that grants permission to the object types, tasks, and custom groups required for operations personnel. This role can then be assigned to your operations users.

Steps to create a custom role for your operations personnel:

1. From the **User Management** dashboard, select the **Roles** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New Role** wizard is started.
3. On the Welcome page of the **New Role** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, select **New based on**. Click the drop-down list for the based on role and select *Operator Tasks*. (Roles are listed in alphabetic order. You can type the start of the role name in the box to narrow down the number of roles and make it easier to find your desired role for selection.) In the Role Details section, enter *Operators* in the Name field. Optionally, enter meaningful text in the Description field to describe your role, and then click **Next**.
5. On the Tasks page, notice that the tasks from the system default role *Operator Tasks* are preselected. In addition to those tasks, select any other tasks you would like your operators to perform. As an example, select the row for *Customize/Delete Activation Profiles*. You can type *customize/* in the filter box to narrow the table to your desired selection, or you can scroll down to find the selection. When you've made all your task selections, click **Next**.
6. On the Objects by Type page, select the rows for the following object types:
   - *Defined CPC*
   - *LPAR Image*
   - *Pattern Match Group*
   - *User-defined Group*.

   Additionally, select any other desired object types, then click **Next**.
7. On the Specific Objects page, select any desired specific objects, then click **Next**.

8. On the Groups page, if any custom groups are available, select any desired custom groups you want your operators to be able to manage, then click **Next**. This page grants Group Management permission (ability to manage to the group, but not to manage the objects in the group).
9. On the Objects by Group page, if any custom groups are available, select any desired groups containing objects for which you want your operators to have permission, then click **Next**. This page grants Child Management permission (ability to manage the objects in the group, but does not grant permission to manage the group). You can click on the group name links to view the current contents of the group.
10. Review the details on the Summary page, then click **Finish**. The role *Operators* is created.
11. On the dashboard, the role *Operators* is added to the list of roles and is the current selected role. View the *Summary for Operators* to verify the Groups, Tasks, Object Types, and Object that the role granted permission are correct.

The role *Operators* can now be assigned to your operations personnel users.

Create a user who authenticated using an LDAP server

If you want to create users that authenticate using your Lightweight Directory Access Protocol (LDAP) server, you first need to create an LDAP server definition. Then you can specify LDAP authentication when you create your users.

Steps to create an LDAP server definition:

1. From the **User Management** dashboard, select the **LDAP Server Definitions** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New LDAP Server Definition** wizard is started.
3. On the Welcome page of the **New LDAP Server Definition** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, keep the default option **New**. In the Server Details section, enter *xyz-ldap* in the Name field. Optionally, enter meaningful text in the Description field to describe your server, then click **Next**.
5. On the Host Connection page, enter the name or IP address of your server in the Primary host name field. Specify any other appropriate selections as needed, then click **Next**.
6. On the Bind Information page, optionally supply appropriate bind credentials.
7. On the Directory Location page, select how to locate a user's directory entry. For example, select **Use DN pattern** and enter *uid={0},type=user,o=xyz.com* in the Pattern field, then click **Next.**
8. Review the details on the Summary page, then click **Finish**. The LDAP server definition xyz-ldap is created.

Steps to create the new user using LDAP authentication:

1. From the **User Management** dashboard, select the **Users** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New User** wizard is started.
3. On the Welcome page of the **New User** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, keep the default option **New**. In the User Details section, enter *Terry* in the Name field. Optionally, enter meaningful text in the Description field to describe your user, then click **Next**.
5. On the Authentication page, select **LDAP password authentication**. Click the drop-down list for the Server and select *xyz-ldap*. Optionally, enter an LDAP user ID in the User ID field, then click **Next**.
6. On the Roles page, select the desired roles for your user, then click **Next**.

Note: You can click on the links for the roles to open **Role Details** for that role. If desired, you can make modifications to user-defined roles from **Roles Details**.

7. Review the details on the Summary page, then click **Finish**. The user Terry is created.
8. On the dashboard, user *Terry* is the current selected user. *View the Summary for Terry* to see the Roles, Groups, Tasks, Object Types, and Objects that Terry is granted permission.

Terry is now able to logon to the console with user ID *Terry* and password specified in the xyz-ldap server. Terry cannot change the password via the console.

Authenticate all employees using an LDAP server

To grant console access to all employees at xyz.com using your Lightweight Directory Access Protocol (LDAP) server, you first need to create an LDAP server definition. Then create a user template defining the settings and permissions for your users. Finally, create a user pattern specifying the specific string pattern used to identify the specific authorized users.

Steps to create an LDAP server definition:

1. From the **User Management** dashboard, select the **LDAP Server Definitions** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New LDAP Server Definition** wizard is started.
3. On the Welcome page of the **New LDAP Server Definition** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, keep the default option **New**. In the Server Details section, enter *xyz-ldap* in the Name field. Optionally, enter meaningful text in the Description field to describe your server, then click **Next**.
5. On the Host Connection page, enter the name or IP address of your server in the Primary host name field. Specify any other appropriate selections as needed, then click **Next.**
6. On the Bind Information page, optionally supply appropriate bind credentials.
7. On the Directory Location page, select how to locate a user's directory entry. For example, select **Search a DN tree** and enter *ou=xyzpages,o=xyz.com* in the DN field. Enter *mail={0}* in the Search filter field, then click **Next**.
8. Review the details on the Summary page, then click **Finish**. The LDAP server definition xyz-ldap is created.

Steps to create a user template:

1. From the **User Management** dashboard, select the **User Templates** icon () in the navigation area.
2. Select the **New** icon (). The **New User Template** wizard is started.
3. On the Welcome page of the **New User Template** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, keep the default option **New**. In the User Template Details section, enter *xyz-template* in the Name field. Optionally, enter meaningful text in the Description field to describe your user template, then click **Next**.
5. On the Authentication page, select the *xyz-ldap* server row from the table, then click **Next**.
6. On the Roles page, select the desired roles for your users, then click **Next**.

   Note: You can click on the links for the roles to open **Role Details** for that role. If desired, you can make modifications to user-defined roles from **Role Details**.
7. Review the details on the Summary page, then click **Finish**. The user template xyz-template is created.

Steps to create the user pattern:

1. From the **User Management** dashboard, select the **User Patterns** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New User Pattern** wizard is started.
3. On the Welcome page of the **New User Pattern** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, keep the default option **New**. In the Pattern Details section, enter *xyz-template* in the Name field. Optionally, enter meaningful text in the Description field to describe your user pattern, then click **Next**.
5. On the User Pattern page, select **Regular expression**. Optionally, click **Help** for details on use of regular expressions. Enter *.*@xyz.com* in the User pattern field, then click **Next**.
6. On the Template page, select the template *xyz-template*, then click **Next**.
7. Review the details on the Summary page, then click **Finish**. The user pattern xyz.com is created.

All user IDs ending in @xyz.com are now able to logon to the console with their LDAP user ID and password. Users are automatically created with the settings and permissions specified in the user template. For example, employee John Doe logs on with user ID johndoe@xyz.com using his LDAP password and then has permission to all roles specified in the xyz-template.

Verify who has permission to a task (for example, the Activate task)

To make sure you have granted the desired roles and users permission to a specific task, you can use the **Tasks** link on the **User Management** dashboard Roles view. The following example looks at the **Activate** task.

Steps to ensure you have the desired permission to the **Activate** task:

1. From the **User Management** dashboard, select the **Roles** icon () in the navigation area.
2. In the **View by**: title, select the **Tasks** link. The dashboard view switches to list all tasks that can have customized permissions.
3. Select the **Activate** task in the objects list.
4. In the *Summary for Activate*, view the list of Users and User Templates that have access permission to the task and the set of Roles that contain the task.

Verify who has access to a specific object

To make sure that you have granted the desired roles and users permission to a specific object, you can use the **Objects** link on the **User Management** dashboard Roles view. The following example looks at the SYS_A object.

Steps to ensure you have the desired permission to the SYS_A object:

1. From the **User Management** dashboard, select the **Roles** icon () in the navigation area.
2. In the **View by**: title, select the **Objects** link. The dashboard view switches to list all of the current system objects that can have customized permissions.
3. Select the SYS_A object in the objects list (scroll down if needed).
4. In the *Summary for SYS_A*, view the list of Users and User Templates that have access permission to the object and Roles that contain the object. You can also see which Tasks can be performed on this object.

Ensure all users are following your security standards for passwords

The **User Management** Password Rules view of the dashboard shows the list of password rules that can be assigned to users. The system defined password rules are Basic, Standard, and Strict. You can create your own customized password rules for your specific security requirements. In the example, the

password needs to be changed every 90 days and must be 8 to 16 characters beginning with a letter. The password is case sensitive and must also contain a number and a special character.

Note: User-defined password rules are case sensitive by default. If you desire to have case insensitive passwords, you can use the **Password Rule Details** task and change the setting for the **Case sensitive** field.

Steps to create a customized password rule:

1. From the **User Management** dashboard, select the **Password Rules** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New Password Rule** wizard is started.
3. On the Welcome page of the **New Password Rule** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, keep the default option **New**. In the Password Rule Details section, enter *xyz-rules* in the Name field. Optionally, enter meaningful text in the Description field to describe your password rule, then click **Next.**
5. On the Password Rules page, select **Expiration (days)**. Enter 90 in the Expiration (days) field. Enter 8 in the Minimum length field. Enter 16 in the Maximum length field. Optionally, customize any other settings on the page, then click **Next**.
6. On the Character Rules page, select **Add** in the **Actions** drop-down list. The Edit Character Rule dialog opens.
7. On the Edit Character Rule dialog, leave the Minimum length 1 and Maximum length 1. In the drop-down list for Alphabetic characters select **Required**. This character rule ensures that the password must start with an alphabetic character. Click **OK**. Your character rule is now in the table.
8. Again, on the Character Rules page, select **Add** in the **Actions** drop-down list. The Edit Character Rule dialog opens.
9. On the Edit Character Rule dialog, change the Minimum length to 7 and Maximum length to 15. In the drop-down list for Alphabetic characters select **Allowed**. In the drop-down list for Numeric characters select **Required**. In the drop-down list for Special characters select **Required**. This character rule ensures that the password must have at least one numeric character and at least one special character. Click **OK**. Your second character rule is now in the table. Click **Next**.
10. Review the details on the Summary page. Click **Finish**. The password rule xyz-rules is created.

Steps to assign the password rule to each of your existing users:

1. From the **User Management** dashboard, select the **Users** icon () in the navigation area.
2. Select the first user you want to customize in the list and select the **Details** icon (). The **User Details** task is opened.
3. Click the Authentication section. Under the Local Authentication radio button, select *xyz-rules* in the Password rule drop-down list.
4. Select the **Force user to change the password at the next logon** check box. This ensures that the next time the user logs on with their current password, the user must create a new password following your security rules. Otherwise, the user is not required to change the password at their next logon even if the password does not conform to the new password rule.
5. Click **OK** on the **User Details** task. The user is updated with the new password rule.
6. On the dashboard, in the Summary for your user, the Authentication section reflects the xyz-rules password rule is in effect.
7. Repeat the above steps for each of your existing users.

Note: As the administrator, you are not required to change the password when you change to a new password rule. Thus, the user is responsible for creating the password that follows the new password rule the next time the password is changed.

Separate system resources between users

If you want to separate system resources between users, you create roles containing the different objects and then assign the appropriate roles to the users. For this example, we have two LPARs on system SYS_A. User Zoey is assigned LPAR image LP01 and user Paul is assigned LPAR image LP02.

Steps to create custom roles for the LPAR image objects:

1. From the **User Management** dashboard, select the **Roles** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New Role** wizard is started.
3. On the Welcome page of the **New Role** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, keep the default option **New**. In the Role Details section, enter *LP01* in the Name field. Optionally, enter meaningful text in the Description field to describe your role, then click **Next**.
5. On the Tasks page, click **Next**.
6. On the Objects by Type page, click **Next**.
7. On the Specific Objects page, enter *lpar image* in the filter box. The table of objects is filtered to show only rows containing text *LPAR Image*. Thus, the view is now limited to all the LPAR images currently on the system. Since our role requires access to just a single LPAR, select the check box on the row with name *LP01* and system *SYS_A*, then click **Next**.
8. On the Groups page, click **Next.**
9. On the Objects by Group page, click **Next.**
10. Review the details on the Summary page, then click **Finish**. The role LP01 is created.
11. On the dashboard, role *LP01* is the current selected role. View the *Summary for LP01* to verify the Objects that role LP01 is granted permission. The Objects section should show object SYS_A:LP01.
12. Repeat the above steps to create the role named *LP02* for LPAR image LP02.

Steps to assign the custom roles to users:

1. From the **User Management** dashboard, select the **Users** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New User** wizard is started.
3. On the Welcome page of the **New User** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, keep the default option **New**. In the User Details section, enter *Zoey* in the Name field. Optionally, enter meaningful text in the Description field to describe your user, then click **Next.**
5. On the Authentication page, keep the default selection **SE password authentication**. Leave the Password rule as the default *Standard*. Enter *zoeypw* as the password in the Password and Confirm password fields. Ensure **Force user to change the password at next logon** is selected, then click **Next**.
6. On the Roles page, enter *LP* in the filter. The table is filtered to show LP01 and LP02 roles. Select the check box on row *LP01*. Clear the filter box and scroll the table to locate *Operator Tasks*. Select the check box on row *Operator Tasks*. Note that the bottom of the table indicates you have *Selected: 2*. Click **Next.**

Note: You can click on the links for the roles to open **Role Details** for that role. If desired, you can make modifications to user-defined roles from **Role Details**.

7. Review the details on the Summary page, then click **Finish.** The user Zoey is created.
8. Again, from the dashboard, select the **New** icon ( ). The **New User** wizard is started.
9. On the Welcome page of the **New User** wizard, click **Next**.
10. On the Name page, in the Create Option section, select **New based on**. Click the drop-down list for the based on user and select *Zoey*. In the User Details section, enter *Paul* in the Name field. Optionally, enter meaningful text in the Description field to describe your user, then click **Next**.
11. On the Authentication page, enter *paulpw* as the password in the Password and Confirm password fields, then click **Next**.
12. On the Roles page, scroll the table to locate LP01. Note that it is preselected from user Zoey. Clear the check box for that role, and select the check box for role LP02. Note that the bottom of the table indicates you have *Selected: 2*. *Operator Tasks* is preselected from user Zoey. Click **Next**.
13. Review the details on the Summary page, then click **Finish**. The user Paul is created.
14. On the dashboard, user *Paul* is the current selected user. View the *Summary for Paul* to verify the Roles are *LP02* and *Operator Tasks*. Also verify Objects is limited to SYS_A:LP02.
15. On the dashboard, select user *Zoey* and repeat the previous step for user *Zoey* to verify she has access to LP01.

Zoey and Paul are now able to logon to the console with their respective user IDs and passwords. They are required to change the password on their first logon. Zoey has access to SYS_A:LP01 and can perform all operator tasks on that LPAR. Similarly, Paul has access to SYS_A:LP02 and can perform all operator tasks on that LPAR.

Assign view only variant of a task to a user (for example, the Hardware Messages task)

There are several view only variants of tasks that you might want to assign to your users (for example: Configure On/Off, Hardware Messages, Operating System Messages, and Advanced Facilities. In this scenario, the **Hardware Messages (view only)** task is assigned to user Terry.

Steps to create a customized role for the **Hardware Messages (view only)** task:

1. From the **User Management** dashboard, select the **Roles** icon ( ) in the navigation area.
2. From the action icons, select the **New** icon ( ). The **New Role** wizard is started.
3. On the Welcome page of the **New Role** wizard, read the text, then click **Next.**
4. On the Name page, in the Create Option section, keep the default option **New**. In the Role Details section, enter *Hardware Messages view only* in the Name field. Optionally, enter meaningful text in the Description field to describe your role, then click **Next**.
5. On the Tasks page, enter Hardware Messages in the filter. The list of tasks is filtered to only show Hardware Messages. Select the check box on the row for *Hardware Messages*, then click **Next**.
6. On the Objects by Type page, click **Next**.
7. On the Specific Objects page, click **Next**.
8. On the Groups page, click **Next**.
9. On the Objects by Group page, click **Next.**
10. Review the details on the Summary page, then click **Finish**. The role *Hardware Messages view only* is created.

Steps to add the customized role to user Terry:

1. From the **User Management** dashboard, select the **Users** icon () in the navigation area.
2. Select the user Terry in the list and select the **Details** icon (). The **User Details - Terry** task is opened.
3. Click the Roles page. Select **Add Roles** in the **Actions** drop-down list. The Add Roles dialog is opened.

   Note: You can click the links for the roles to open **Role Details** for that role. If desired, you can make modifications to user-defined roles from **Role Details**.
4. On the Add Roles dialog, enter *view only* in the filter. Select the check box in the *Hardware Messages view only* row, then click **OK**. The role is added to the list of roles for the user.
5. Click **OK** on the **User Details** task. The user Terry is updated with the additional role.
6. On the dashboard, in the *Summary for Terry*, the Roles section includes the new role and the Tasks section contains the **Hardware Messages (view only)** task.

Create a customized managed object role (similar to the approach available in HMC version 2.12.1)

For administrators who are familiar with the **Customize User Controls** task in HMC version 2.12.1, this scenario guides you through creating a customized managed object role (formerly managed resource role) using the **User Management** task. For this example, we copy the HMC system defined role *Defined System Managed Objects* (formerly *Defined zCPC Managed Objects*) to create a new role that has access to defined systems and undefined systems (whereas normally the access is limited to defined systems). When assigned to a user, the new role would grant permission to view systems currently managed by the HMC, and systems that could be managed by the HMC if added by the **Add Object Definition** task. Separate role permission is needed for the user to have permission to the **Add Object Definition** task.

Steps to create a custom role for the Defined System Managed Objects:

1. From the **User Management** dashboard, select the **Roles** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New Role** wizard is started.
3. On the Welcome page of the **New Role** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, select **New based on**. Click the drop-down list for the based on role and select *Defined System Managed Objects*. (Roles are listed in alphabetic order. You can type the start of the role name in the box to narrow down the number of roles and make it easier to find your desired role for selection.) In the Role Details section, enter *Defined and Undefined System Managed Objects* in the Name field. Optionally, enter meaningful text in the Description field to describe your role, and then click **Next**.
5. Since we are creating a role specific for objects, on the Tasks page, click **Next**.

   Note: With the **User Management** task, a role can contain a mixture of objects (resources) and tasks, whereas the **Customize User Controls** task required separate roles. Therefore, if desired, you could grant permission to the **Add Object Definition** task at this point.
6. On the Objects by Type page, notice that there are object types preselected from *Defined System Managed Objects* role. Leave all the preselected object types. Additionally, select the row for *Undefined CPC*, and then click **Next**.
7. On the Specific Objects page, click **Next**.
8. On the Groups page, click **Next**.
9. On the Objects by Group page, click **Next**.
10. Review the details on the Summary page, then click **Finish**. The role *Defined and Undefined System Managed Objects* is created.

11. On the dashboard, role *Defined and Undefined System Managed Objects* is the current selected role. View the *Summary for Defined and Undefined System Managed Objects* to verify the Object Types that the role granted permission are correct.

Note: When creating a name longer than the designated name length in the objects list, a scroll bar is displayed at the bottom of the object list area for you to scroll to view the entire name.

The role *Defined and Undefined System Managed Objects* can now be assigned to desired users.

Create a customized task role (similar to the approach available with HMC version 2.12.1)

For administrators who are familiar with the **Customize User Controls** task in HMC version 2.12.1, this scenario guides you through creating a customized task role using the **User Management** task. For this example, we copy the HMC system defined role *Operator Tasks* to create a new role that adds permission to customize activation profiles. When assigned to a user, the new role would grant permission to operators to modify and delete activation profiles, whereas normally they are limited to viewing activation profiles.

Steps to create a custom role for the Operator Tasks:

1. From the **User Management** dashboard, select the **Roles** icon () in the navigation area.
2. From the action icons, select the **New** icon (). The **New Role** wizard is started.
3. On the Welcome page of the **New Role** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, select **New based on**. Click the drop-down list for the based on role and select *Operator Tasks*. (Roles are listed in alphabetic order. You can type the start of the role name in the box to narrow down the number of roles and make it easier to find your desired role for selection.) In the Role Details section, enter *Operator Tasks with Activation Profiles* in the Name field. Optionally, enter meaningful text in the Description field to describe your role, then click **Next**.
5. On the Tasks page, notice that there are tasks preselected from *Operator Tasks* role. Use the scroll bars as needed to select the row for *Customize/Delete Activation Profiles*, clear the check box on the row for *View Activation Profiles*, and then click **Next**.
6. On the Objects by Type page, click **Next**.
7. On the Specific Objects page, click **Next**.
8. On the Groups page, click **Next**.
9. On the Objects by Group page, click **Next**.
10. Review the details on the Summary page, then click **Finish**. The role *Operator Tasks with Activation Profiles* is created.
11. On the dashboard, role *Operator Tasks with Activation Profiles* is the current selected role. View the *Summary for Operator Tasks with Activation Profiles* to verify the Tasks that the role granted permission are correct.

The role *Operator Tasks with Activation Profiles* can now be assigned to desired users.

Create an HMC user for OSA/SF

In order to utilize the Open System Adapter/Support Facility (OSA/SF) configuration windows on your Hardware Management Console, the HMC access administrator must create a user for the OSA/SF system administrator. This new user has the required permissions for the objects and tasks required on the HMC for the OSA/SF system administrator.

Steps for the HMC access administrator to create a custom role for your OSA/SF system administrator are as follows:

1. From the **User Management** dashboard, select the **Roles** icon in the navigation area.
2. From the actions icons, select the **New** icon. the **New Role** wizard is started.

3. On the Welcome page of the **New Role** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, leave the selection **New**. In the Role Details section, enter *OSASF Tasks* in the Name filed. Optionally, enter meaningful text (that is, *OSA Support Facility tasks*) in the Description field to describe your role, and then click **Next**.
5. On the Tasks page, select the **OSA Advanced Facilities** task. You can type *facilities* in the filter to narrow down the list of tasks in the table, or you can scroll down to find the selection. When you have made the task selection, click **Next**.
6. On the Objects by Type page, select the rows for the following object types. When complete, click **Next**.
   a. *Defined CPC*
   b. *LPAR Image*
7. On the Specific Objects page, make no selections, then click **Next.**
8. On the Groups page, make no selections, then click **Next**.
9. On the Objects by Group page, make no selections, then click **Next**.
10. Review the details on the Summary page, then click **Finish**. The role *OSASF Tasks* is created. On the dashboard, the role *OSASF Tasks* is added to the list of roles and is the current selected role. View the *Summary for OSASF Tasks* to verify the Tasks and Object Types that the role granted permission are correct.

Steps to create the user for the OSA/SF system administrator are as follows:

1. From the **User Management** dashboard, select the **Users** icon in the navigation area.
2. From the actions icons, select the **New** icon. The **New User** wizard is started.
3. On the Welcome page of the **New User** wizard, read the text, then click **Next**.
4. On the Name page, in the Create Option section, leave the selection **New**. In the User Details section, enter *OSASF* in the Name field. Optionally, enter meaningful text (that is, *OSA Support Facility user*) in the Description field to describe your user, and then click **Next**.
5. On the Authentication page, keep the default selection **SE password authentication**. Leave the Password rule as the default *Standard*. Enter the desired password in the Password and Confirm password fields, then click **Next**.
6. On the Roles page, select the check box for role *OSASF Tasks* to give the user access to the required objects and tasks. You can type *osa* in the filter to narrow down the list of roles in the table, or you can scroll down to find the selection. When you have made the task selection, click **Next**.
7. Review the details on the Summary page, then click **Finish**. The user *OSASF* is created.
8. On the dashboard, user *OSASF* is added to the **Users** list and is the current selected users. View the *Summary for OSASF* to see the Roles, Tasks, and Object Types that OSASF is granted permission

For more information on using the OSA/SF on the Hardware Management Console, see the *Open System Adapter/Support Facility on the Hardware Management Console*, SC14-7580.

Default Permissions

The system grants every user permission to certain tasks, groups, objects, and object types. These specific permissions cannot be set up or removed by the **User Management** task. Therefore, the access administrator is not required to manage these permissions.

The list of default permissions provided to every user is as follows:

- Tasks
  - Details tasks as follows:
    - Image Details
    - System Details

    Note: The Details tasks are the read only version and might limit the information displayed.

  - Change Password
  - Logoff or Disconnect
  - User Management (This is limited to the Users navigation and only for viewing or updating specific settings for the current user.)
- Groups
  - All system defined managed object groups (such as Systems Management). Note that a system defined managed object group does not display in the Navigation Pad unless the logged on user has permission to one or more objects contained in that managed object group.
  - All system defined task lists (such as Daily, etc.). Note that a task list does not display in the Tasks Pad unless the logged on user had permission to one or more tasks contained in that task list.
- Objects
  - Console object
- Object Types (on the Hardware Management Console only)
  - Fibre Channel Network
  - Hardware Management Console
  - HMC Optical Network

Users

This task is used by an access administrator or a user that is assigned a role with Manage Users task permission. A *user* is a combination of a user name (user ID), permissions, authentication mode, and a text description. Permissions represent the authority levels that are assigned to the user for the objects and tasks the user has permission to access.

The user ID and password are used to verify a user's authorization to log on to the console. The password is determined by the password rule that is chosen for the user. The default choices are *Basic*, *Strict*, and *Standard*, however, other rules may also be available if they were defined in the **Password Rules** task. All these rules have their own set of specifications for assigning a password. Your access administrator determines what password rule is appropriate for you, whether you must change your password at the next logon, and whether you can log on to the console locally or remotely.

Use this task to choose the type of password authentication you want to assign to a user. If you choose the **SE password authentication**, then the password authentication is performed by using the console. If you choose the **LDAP password authentication**, then the password authentication is delegated to an LDAP server. You use the **LDAP Server Definitions** task to define the LDAP server. You can also enable multi-factor authentication for a user that requires the user to log on to the console with additional requirements.

The user definition specifies roles that are assigned to the user. You can choose from a list of available default roles or create user-defined roles using the **New Role** task. A role defines permissions to tasks, types of objects or specific objects, groups, and task lists.

The system contains the following predefined default users:

- ACSADMIN
- SERVICE

You cannot change the roles of the default users. You can create a new user based on the desired system default user and modify the roles for the new user.

Attention: The use of default passwords are no longer allowed. The first time a default user ID logs on to the console, the default password must be changed. A prompt is displayed requiring the password change.

This password default change is controlled by SERVICE or a user that is assigned a role with Manage Users task permission by selecting **Default Users** from the **Users** view and then clicking the **Details** icon. The Change default user passwords prompt is displayed. If you are using a user that is assigned a role with Manage Users task permission, then each default user's password is reset to its default value and all default users are required to change their passwords the next time they log in. If you are using SERVICE, then only that password is reset to the default and all default users are required to change their passwords the next time they log in.

The **Users** dashboard view displays a list of all currently defined users with user summary sections as follows:

General
This section contains the description, last logon, and disabled fields for the selected user.

Authentication
This section contains the authentication type and corresponding authentication settings.

Roles
This section lists all of the role permissions that are assigned to the selected user.

Groups
This section lists all of the user-defined custom groups (including pattern match groups) that the selected user has Group Management permission to modify. Groups that the user is granted only Child Management permission are not shown.

Tasks
This section lists all of the tasks the selected user is granted permission by the assigned roles. The list does not include tasks that the user has available by "Default Permissions" on page 888.

Object Types
This section lists all of the types the selected user is granted permission by the assigned roles. The list does not include object types that the user has available by "Default Permissions" on page 888.

Objects
This section lists all the objects the user is granted permission to access by the assigned roles. Permission has been granted in a role by either object type, specific object, or Child Management permission to a group. The list does not include objects that the user has available by "Default Permissions" on page 888.

You can view the object summary using the **Expand** and **Collapse** icons to view or hide sections. You can create a new user definition using the **New User** wizard or manage an existing user definition with **User Details**.

- Click the **"New User" on page 890** () icon to create a new user definition. When the **New User** wizard completes, the new user is added to the Users list.

- Click the **"User Details" on page 893** () icon to manage an existing user definition. You cannot modify the roles specified in the system defined default users. You can also use this icon with **Default Users** to reset the passwords of the default user IDs.

- Click the **Delete** () icon to delete an existing user definition. You can delete system default users, but be sure you have created new customized users based on these system default users before deleting.

New User

Use the **New User** wizard to guide you through creating a new user. The **New User** wizard is organized into the following pages, each page of which is listed on the left navigation. The currently displayed page is highlighted. Use the Filter function to enter a filter string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

- Use the “Name” on page 891 page to specify the user name, along with an optional description and email address. It also provides capability to create a new user or copy an existing user.
- Use the “Authentication” on page 892 page to select an authentication type for the new user.
- Use the Roles page to select one or more roles to define access permissions for this new user. You can click on the links for the roles to open **Role Details** for that role. If desired, you can make modifications to user-defined roles from **Roles Details**.
- Use the Summary page to view a summary report of the new user to be created. When you click **Finish**, the new user is created and populated with the values specified in the **New User** wizard.

The **New User** wizard displays the Welcome page when you start the task for the first time. This page provides a summary of the steps that you will complete to create your new user. Select **Show this welcome page next time** to clear the box if you do not want to display the Welcome page next time you use the **New User** wizard.

Additional functions on this window include:

Back
To navigate to the previous page in the wizard, click **Back**.

Next
To navigate to the next page in the wizard, click **Next**.

Finish
To create the new user, click **Finish**.

Cancel
To exit the wizard without creating the new user, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

Name

Use the Name page to enter a name and optional description for the new user you want to create. After entering the information, click **Next** to proceed to the next page.

Create Option
This option determines how the object is created.

New:
Create a new user.

New based on:
Select an existing user to base the new user on. The settings in the new user are initialized to those of the existing user. The system default users are as follows:

- ACSADMIN
- SERVICE

Note: You cannot change the roles of the default users.

If you want the ability to change the roles for a default user, create your own version by copying an existing default user.

User Details
This section requires a name and an optional description.

Name:
Specify the user name for the user you are creating. When creating a new user, the user name can be 4 to 320 characters in length and a combination of upper and lower-case letters (A-Z, a-z), numbers (0-9), and the following special characters:

- back slash (\)
- greater than (>)

- less than (<)
- asterisk (*)
- ampersand (&)
- question mark (?)
- apostrophe (')
- comma (,)
- colon (:)
- left and right parentheses ( )
- semicolon (;)
- number sign (#)
- percent sign (%)
- equals sign (=)
- plus sign (+)
- dash (-)
- underscore (_)
- at sign (@)
- slash (/)
- period (.)

The name must be unique among existing user names. The comparison for duplicate name is case insensitive.

Description:
Specify an optional meaningful text that describes your user. The description can be up to 1024 characters with no character restrictions.

Email Address:
Enter an optional, valid email address for this user.

Authentication

Use the Authentication page to select the password authentication you want to assign to the new user.

Password authentication and password rules

If you choose the **SE password authentication**, then the password authentication is performed by using the console. If you choose the **LDAP password authentication**, then the password authentication is delegated to an LDAP server. After entering the information, click **Next** to proceed to the next page.

Choose the password authentication that you want by selecting one of the following:

- Select **SE password authentication** to perform password authentication by using the console.

Password rule:
You must select a password rule to be used for the specified new user. Click the drop-down arrow for a list of rules, then select one. The system defined default password rules are as follows:

Basic
The basic password rules consist of:

– A password must be a minimum of four characters and a maximum of eight characters long.
– These characters include A-Z, a-z, 0-9.

Standard
The standard password rules consist of:

– Password expires in 186 days.

- A password must be a minimum of six characters and a maximum of 30 characters long.
- The first and last character in a password can be alphabetic or special.
- A password can contain letters, numbers, and special characters.
- No character can repeat more than twice.
- A password can only match three characters from the previous password.
- You can repeat a password after using four unique passwords.

Strict
The strict password rules consist of:

- Password expires in 180 days.
- A password must be a minimum of six characters and a maximum of eight characters long.
- A password must contain both letters and numbers.
- The first and last character in a password must be alphabetic.
- No character can repeat more than twice.

Password:
Specify the password for the new user. Follow the password rule specified in the Password rule field.

Confirm password
Specify the password again for verification.

Select **Force user to change the password at next logon** to specify whether the user should be forced to change the password the next time the log in to the console.

- Select **LDAP password authentication** to delegate password authentication to an LDAP server.

Server
You must specify an LDAP server to be used for the new user. Click the drop-down arrow for a list of LDAP servers, then select one. Use the “LDAP Server Definitions” on page 927 dashboard view to create and manage LDAP server definitions.

User ID
Specify an optional LDAP user ID if it is different from the new user name.

Multi-factor authentication (MFA)

- Select **No MFA**, if this user is not required to use multi-factor authentication when logging on to the console.
- Select **SE MFA** to require this user to use the console's TOTP authentication when logging on to the console.

User Details

Use the **User Details** task to view and manage the properties of a selected user. Use the navigation links on the left to display each tab or use the **Expand All** and **Collapse All** icons to display each section view.

- Select the “General” on page 894 navigation link or the **Expand** icon to display the General details tab section.
- Select the “Session” on page 894 navigation link or the **Expand** icon to display the Session details tab section.
- Select the “Authentication” on page 895 navigation link or the **Expand** icon to display the Authentication details tab section.
- Select the **Roles** navigation link or the **Expand** icon to display the Roles details tab section. Use the **Actions** menu to “Add Roles” on page 897 or Remove Roles defining access permission for the user. You can click the links for the roles to open **Role Details** for that role. If desired, you can make modification to user-defined roles from **Role Details**.

You can also use **User Details** when you select **Default Users** to reset the default user ID default passwords.

Additional functions on this window include:

OK
To save the current changes and exit the task, click **OK**.

Apply
To save the current changes for the user without exiting the task, click **Apply**.

Cancel
To exit the window, click **Cancel**. A confirmation window is displayed. The information that you entered is not saved.

Help
To display help for the current window, click **Help**.

General

Use the General details tab section to view the name and modify the description and other settings for the user.

Name:
Specifies the name for the user you are modifying.

Description:
Specify an optional meaningful text that describes your user.

Email address:
Enter an optional, valid email address for this user.

Object ID:
Specifies the associated Universal Unique Identifier (UUID) of the managed object.

Note: This value cannot be modified.

Default group:
The "Default Group" on page 896 specifies a group to which any objects created by the user will be added by default. Select a group or **No default group** from the drop-down list. Be sure that the user has Group Management permission to the group selected.

Disable user
Indicates that you want to disable the user from logging into the console. A user is not allowed to disable their own user.

Note: This option changes to **Disabled due to inactivity** when the amount of days specified in the **Disable for inactivity (days)** has been exceeded.

Disabled due to inactivity
Indicates that the user's inactivity has exceeded the amount of days specified in the **Disable for inactivity (days):** option. Select **Disabled due to inactivity** to remove the check and re-enable the user.

Session

Use the Session details tab section to view or modify the interval, in minutes, the user's session can run before being prompted for identity verification.

Note: If you use the **Single Object Operations** task from the Hardware Management Console, the session timeout is disabled on the Support Element for the duration of the Single Object Operations session.

Session timeout (minutes):
Select this to specify the interval, in minutes, over which a user's session can run before being prompted for identity verification. If a value other than zero is specified, the user is prompted after the specified minutes have been reached to re-enter their password. If a password is not re-entered within the amount of time that was specified in the *Verify timeout minutes* field, then the session is

disconnected. You can specify up to a maximum value of 525600 minutes (equivalent to one year). There is no expiration when unselected.

Verify timeout (minutes):
Select this to specify the amount of time that is required for the user to re-enter their password when prompted, if a value was specified in the *Session timeout minutes* field. If the password is not re-entered within the specified time, the session will be disconnected. The default is 15 minutes. You can specify up to a maximum value of 525600 minutes (equivalent to one year). There is no expiration when unselected.

Idle timeout (minutes):
Select this to specify the number of minutes the user's session can be idle. If the user does not interact with the session in the specified amount of time, the session will be disconnected. You can specify up to a maximum value of 525600 minutes (equivalent to one year). There is no expiration when unselected.

Authentication

Use the Authentication details tab section to view or modify the method of authenticating the user.

Password authentication and password rules

- To perform password authentication by using the console, select **SE password authentication**.

  Password rule:
  You must select a password rule to be used for the specified user. Click the drop-down arrow for a list of rules, then select one. The system defined default password rules are as follows:

  Basic
  The basic password rules consist of:

  – A password must be a minimum of four characters and a maximum of eight characters long.
  – These characters include A-Z, a-z, 0-9.

  Standard
  The standard password rules consist of:

  – Password expires in 186 days.
  – A password must be a minimum of six characters and a maximum of 30 characters long.
  – The first and last character in a password can be alphabetic or special.
  – A password can contain letters, numbers, and special characters.
  – No character can repeat more than twice.
  – A password can only match three characters from the previous password.
  – You can repeat a password after using four unique passwords.

  Strict
  The strict password rules consist of:

  – Password expires in 180 days.
  – A password must be a minimum of six characters and a maximum of eight characters long.
  – A password must contain both letters and numbers.
  – The first and last character in a password must be alphabetic.
  – No character can repeat more than twice.

  Password:
  Specify the password for the user. Follow the password rule specified in the Password rule field.

  Confirm password
  Specify the password again for verification.

- To delegate password authentication to an LDAP server, select **LDAP password authentication**.

Server
You must specify an LDAP server definition to be used for the user. Click the drop-down arrow for a list of LDAP servers, then select one.

User ID
Specify an optional LDAP user ID if it is different from the user name.

- To require the user to change their password the next time they log on to the console, click **Reset**.
- Select **Delay login after failed attempts** to enable the login delay for continual invalid login attempts.

  Number of failed attempts before disable delay
  Specify the number of failed attempts before the user is temporarily disabled from being able to log on.

  Delay (minutes)
  Specify the amount of time in minutes the user is temporarily disabled after reaching the number of failed attempts.
- Select **Disable for inactivity (days):** to specify that a user is disabled if they have not logged on within a specified number of days. Then, specify the number of days after which the inactive user becomes disabled.
- Select **Minimum time between password changes (minutes)** to specify the minimum amount of time in minutes that must elapse between changes for the user's password. Unselected indicates that a user's password can be changed immediately after it has been changed.

  Note: This field is not applicable to a user that has LDAP authentication.
- Select **Require password for disruptive actions** to enable a password requirement, for this user, on a task that causes disruptive actions. This option, by default, is selected.

  Note: This option is disabled for the default SERVICE user. Therefore, the SERVICE user is always required to specify its password before proceeding with a task that causes disruptive actions.
- Select **Require text input for disruptive actions** to enable a text input requirement before performing a disruptive action on an object.

Multi-factor authentication (MFA)

- Select **No MFA**, if this user is not required to use multi-factor authentication when logging on to the console.
- Select **SE MFA** to require this user to use the console's TOTP authentication when logging on to the console.
- To require this user receive a new shared secret key the next time the user logs on to the console, click **Reset**. This option is only available when you select **SE MFA**.

Default Group

Use the Default group field to choose the default group for the user. A *default group* is a user-defined group to which objects created by the user will be added by default. Use the drop-down to choose either **No default group** or select the desired group.

Default group
Choose a group that objects created by the user are added by default. The administrator should ensure that the user has access permission to manage the default group. Select **No default group** if you do not want to have new objects created by the user added to a group.

The default group cannot be a pattern match group since new objects defined by the user might not match the specific pattern for the group. Thus, no pattern match groups are included in the list.

Tasks that result in objects being added to a default group are as follows:

- Grouping

A custom group cannot be deleted if it is designated as the default group for at least one user or user template.

Add Roles

Use this action to select new role permissions to add to the user. You can use the Filter function string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

You can click on the links for the roles to open **Role Details** for that role. If desired, you can make modifications to user-defined roles from **Role Details**.

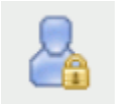
Additional functions on this window include:

OK
To perform the operation, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Roles



This task is used by an access administrator or a user that is assigned a role with Manage User Roles task permission. A ***role*** is a collection of authorizations that define permissions to tasks, type of objects or specific objects, groups, and task lists. A role can be created to define the set of tasks and managed objects allowed for a given class of user. Once you have defined or customized the role you can use the **Users** task to create new users with their own permissions.

Use this window to define and customize roles. A role assigns permission to a task or a managed object or group of objects, such as a managed system or logical partition. The **Roles** view can be changed by selecting the **Roles**, **Objects**, and **Tasks** links.

- **“View by Roles” on page 897**
- **“View by Objects” on page 898**
- **“View by Tasks” on page 898**

You can view the object summary using the **Expand** or **Collapse** icons to view or hide sections.

The following actions are only available in the **View by Roles** dashboard view. You can create a new role definition using the **New Role** wizard or manage an existing user definition with **Role Details**.

- Click the **“New Role” on page 899** () icon to create a new role definition. When the **New Role** wizard completes, the new role is added to the Roles list.
- Click the **“Role Details” on page 900** () icon to view or modify an existing role definition. You cannot modify system defined roles.
- Click the **Delete** () icon to delete an existing role definition. You cannot delete system defined roles or roles that are associated with a user or user template.
- Click the **“New Task List” on page 903** () icon to open the **Role Details** task and create a new task list for the selected role. The **New Task List** icon is only available for user-defined roles.

View by Roles

The **View by Roles** dashboard view displays a list of all currently defined roles with role summary sections as follows:

General
A statement describing the selected role.

Users
A list of users who have access to this role.

User Templates
A list of user templates that have access to this role.

Groups
A list of user-defined custom groups (including pattern match groups) granted Group Management permission by the role. Groups which are granted only Child Management permission are not shown.

Tasks
A list of tasks available in the role.

Object Types
A list of object types permitted by the role.

Objects
A list of all objects permitted by the role. It lists any objects the role would grant access by object type, specific object, or Child Management permission to a group.

Task Lists
A list of task lists permitted by the role.

View by Objects

The **View by Objects** dashboard view displays all currently defined and undefined objects on the system that can have permission assigned. The administrator can view roles that contain a particular object.

General
A statement describing the selected object.

Users
An alphabetized list of users who have access to this object.

Tasks
An alphabetized list of tasks that can target this object if the role permits.

Roles
An alphabetized list of roles that contain this object.

View by Tasks

The **View by Tasks** dashboard view displays a list of all system tasks that can have customized permissions. The administrator can view roles and users that have permission to a particular task.

General
A statement describing the selected task.

Users
A list of users who have access to this task.

Groups
A list of user-defined custom groups (including pattern match groups) that are allowable targets for the task. You can launch the task on the children of the custom group by selecting the group in the navigation area, selecting all targets in the table, and then launching the task.

Roles
A list of roles that permit this task.

Object Types
A list of types of objects that are allowable targets for the task.

Objects
A list of objects that are allowable targets for the task.

New Role

Use the **New Role** wizard to guide you through creating a new role. The **New Role** wizard is organized into the following pages. Each page is listed on the left navigation. The currently displayed page is highlighted. Use the Filter function to enter a filter string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

- Use the "Name" on page 899 page to specify the role name and optional description. It also provides capability to create a new role or copy an existing role.
- Use the Tasks page to select the tasks to be included in the new role. The list of tasks contains all system tasks that can have customized permissions.
- Use the Objects by Type page to select the type of objects to include in the role. By adding an object type to the role, all objects of that type, regardless of whether they currently exist or are created in the future, are permitted to users or user templates with the role.
- Use the Specific Objects page to select specific objects to include in the new role. The list of objects contains all currently defined and undefined objects on the system that can have permission assigned.
- Use the Groups page to select groups to include in the new role. Adding a group gives permission to manage the group (Group Management), but does not give permission to objects in the group. The groups listed include all custom groups including pattern match groups. System defined groups such as Defined CPCs are not included.
- Use the Objects by Group page to select a group that contains the objects you want to include in the new role. Adding a group grants permission to objects in the group (Child Management), but does not grant permission to manage the group. You can use the links provided on the group name to view the objects ("Group Resources" on page 900) currently in that group. The groups listed include all custom groups except pattern match groups.
- Use the Summary page to view a summary report of the new role to be created. When you click **Finish**, the new role is created and populated with the values specified in the **New Role** wizard.

The **New Role** wizard displays the Welcome page when you start the task for the first time. This page provides a summary of the steps that you will complete to create your new role. Select **Show this welcome page next time** to clear the box if you do not want to display the Welcome page next time you use the **New Role** wizard.

Additional functions on this window include:

Back
To navigate to the previous page in the wizard, click **Back**.

Next
To navigate to the next page in the wizard, click **Next**.

Finish
To create the new role, click **Finish**.

Cancel
To exit the wizard without creating the new role, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

Name

Use the Name page to enter a name and description for the new role you want to create. After entering the information, click **Next** to proceed to the next page.

Create Option
This option determines how the object is created.

New:
Create a new role

New based on:
Select an existing role to base the new role on. The settings in the new role are initialized to those of the existing role.

Role Details
This section specifies a name and an optional description.

Name:
Specify the name for the new role you are creating. When creating a new role, the name can be 1 to 64 characters in length, cannot begin or end with a space, a combination of upper and lower-case letters (A-Z, a-z), numbers (0-9), and the following special characters:

- period (.)
- hyphen (-)
- at sign (@)
- underscore (_)
- space ( )

The name must be unique among existing role names. The comparison for duplicate name is case insensitive.

Description:
Specify an optional meaningful text describing your role. The description can be up to 1024 characters with no character restrictions.

Associated system defined role:
Defines the role to be used for the **Single Object Operations** (SOO) task. Also, used to enable/disable certain features of the tasks (such as the **Users and Tasks** task).

Group Resources

Displays an informational table listing the objects currently contained in the group.

Additional functions on this window include:

Close
To exit the current window, click **Close**.

Help
To display help for the current window, click **Help**.

Role Details

Use the **Role Details** task to view the role properties of a selected role. Optionally, you can modify properties of a user-defined role. Use the navigation links on the left to display each tab or use the **Expand All** and **Collapse All** icons to display each view. Use the Filter function to enter a filter string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

- Select the "General" on page 901 navigation link or the **Expand** icon to display the General section.
- Select the **Types** navigation link (or the **Expand** icon) to display the Types section. View or modify the role types by using the actions "Add Types to Role" on page 901 or **Remove Types from Role**.
- Select the **Objects** navigation link (or the **Expand** icon) to display the Objects section. View or modify the role objects by using the actions "Add Objects to Role" on page 901 or **Remove Objects from Role**.
- Select the **Tasks** navigation link (or the **Expand** icon) to display the Tasks section. View or modify the role tasks by using the actions "Add Tasks to Role" on page 902 or **Remove Tasks from Role**.
- Select the **Groups** navigation link (or the **Expand** icon) to display the Groups section. View or modify the role groups by using the actions "Add Groups to Role" on page 902 , **Remove Groups from Role**, or "Edit Group Permissions" on page 902.
- Select the **"Task Lists" on page 903** navigation link (or the **Expand** icon) to display the Task Lists section. View or modify the task list using actions New Task List, Task List Details, Delete Task List, Add Tasks to Task List, and Remove Tasks from Task List.

Additional functions on this window include:

OK
To save the current changes and exit the task, click **OK**. This function is available only for user-defined roles.

Apply
To save the current changes for the role without exiting the task, click **Apply**. This function is available only for user-defined roles.

Close
To exit the window, click **Close**. This function is available only for system defined roles since they cannot be modified.

Cancel
To exit the window, click **Cancel**. A confirmation window is displayed. The information you entered is not saved. This function is available only for user-defined roles.

Help
To display help for the current window, click **Help**.

General

Use the General details tab section to modify the description for the selected role.

Name:
Specifies the name of the role you are modifying.

Description:
Specify an optional meaningful text for your role.

Object ID:
Specifies the associated Universal Unique Identifier (UUID) of the managed object.

Note: This field cannot be modified.

Associated system defined role:
Defines the role to be used for the **Single Object Operations** (SOO) task. Also used to enable/disable certain features of the tasks (such as the **Users and Tasks** task).

Add Types to Role

Use this action to add additional object types to the role. The list of object types includes all object types that are not already included in the role. By adding an object type to the role, all objects of that type, regardless of whether they currently exist or are created in the future, are permitted to users or user templates with the role. If all object types are already contained in the role, the message "No items to display" is shown. You can select all types by selecting the top check box.

Use the Filter function to enter a filter string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

Additional functions on this window include:

OK
To perform the operation and save the changes to the role, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Objects to Role

Use this action to add additional objects to the role. The list of objects includes all managed objects that are not already included in the role. If all objects are already contained in the role, the message "No items to display" is shown. You can select all objects by selecting the top check box.

Use the Filter function to enter a filter string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

Additional functions on this window include:

OK
To perform the operation and save the changes to the role, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Tasks to Role

Use this action to add tasks to the role. The list of tasks includes all tasks (that can have permission assigned) that are not already included in the role. If all tasks are already contained in the role, the message "No items to display" is shown. You can select all tasks by selecting the top check box.

Use the Filter function to enter a filter string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

Additional functions on this window include:

OK
To perform the operation and save the changes to the role, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Groups to Role

Use this action to add additional user-defined groups to the role. The list of groups includes all user-defined groups that are not already included in the role. If all groups are already contained in the role, the message "No items to display" is shown. You can select all groups by selecting the top check box. Select the permission type you want to add to the group:

Group management
Grants permission to manage the group, but does not grant permission to objects in the group.

Child management
Grants permission to manage objects in the group, but does not grant permission to the group.

Group and child management
Grants permission to manage the group and permission to the objects in the group.

Note: You cannot assign **Child management** or **Group and child management** to a pattern match group.

Additional functions on this window include:

OK
To perform the operation and save the changes to the role, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Edit Group Permissions

Use this action to edit the group permissions for the selected group. The permission type to select:

Group management
Grants permission to manage the group, but does not grant permission to objects in the group.

Child management
Grants permission to manage objects in the group, but does not grant permission to the group.

Group and child management
Grants permission to manage the group and permission to the objects in the group.

Note: You cannot assign **Child management** or **Group and child management** to a pattern match group.

Additional functions on this window include:

OK
To perform the operation and update the group selection permission, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Task Lists

A *task list* is a grouping of tasks for a defined purpose such as Daily tasks or Configuration tasks. You can create your own custom task lists for your specific purpose. New task lists are displayed in the user interface under the Tasks Pad for users that have permission to the role that defines the task list.

You can also modify system defined task lists to add tasks to the list. For example, you can add the **Integrated 3270 Console** to the Daily task list by creating a new task list with the name Daily and adding the task to the list. The task is added to the Daily list alphabetically. You cannot remove tasks from a system defined task list.

Only groupable tasks can be added to a task list. Console actions tasks or root tasks (such as System Details) cannot be added to a task list.

Use the Task List section to create new task lists or manage existing task lists assigned to the role by using the following actions:

- “New Task List” on page 903
- “Task List Details” on page 904
- Delete Task List
- “Add Tasks to Task List” on page 905
- Remove Tasks from Task List

New Task List

Use this action to create a new task list for the selected role. The table contains the list of groupable tasks contained in the role. You can select all tasks by selecting the top check box. Use the Filter function to enter a filter string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

Name
Specify the name for the new task list you are creating. When creating a new task list, the name can be 1 to 64 characters in length, cannot begin or end with a space, a combination of upper and lower-case letters (A-Z, a-z), numbers (0-9), and the following special characters:

- period (.)
- hyphen (-)
- at sign (@)
- underscore (_)
- space ( )

The name must be unique among existing task list names. The comparison for duplicate name is case insensitive.

Description
Specify an optional meaningful text for your task list. The description can be up to 1024 characters with no character restrictions.

You can work with the table by using the table icons or **Action** list from the table toolbar. If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar:

Export as HTML
Downloads table data into a Hypertext Markup Language (HTML) file. This action is only available when you are using a remote browser.

Export All to CSV
Downloads table data into a Coma Separated Values (CSV) file. You can then import the downloaded CSV file into most spreadsheet applications. This action is only available when you are using a remote browser.

Print All
Prints all rows in the table. This action is only available when you are using a remote browser.

Print Selected
Prints selected rows in the table. This action is only available when you are using a remote browser.

Print Preview
Displays a printable version of all rows in the table. This action is only available when you are using a remote browser.

Configure Options
Selects the columns that you want to display. All available columns are in the list by their column name. Select the columns that you want displayed or hidden by selecting or clearing the items in the list. When you complete the configuration, click **OK**. The columns are displayed in the table as you specified.

Additional functions on this window include:

OK
To perform the operation and create a new Task List, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Task List Details

Use this action to modify the selected task list.

You can work with the table by using the table icons or **Actions** list from the table toolbar. If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar:

Add Tasks to Task List
Adds one or more tasks to the task list.

Remove Task from Task List
After confirmation, removes the select task from the task list. This action is only available if you have selected a task row in the table.

Export as HTML
Downloads table data into a Hypertext Markup Language (HTML) file. This action is only available when you are using a remote browser.

Export All to CSV
Downloads table data into a Coma Separated Values (CSV) file. You can then import the downloaded CSV file into most spreadsheet applications. This action is only available when you are using a remote browser.

Print All
Prints all rows in the table. This action is only available when you are using a remote browser.

Print Selected
Prints selected rows in the table. This action is only available when you are using a remote browser.

Print Preview
Displays a printable version of all rows in the table. This action is only available when you are using a remote browser.

Configure Options
Selects the columns that you want to display. All available columns are in the list by their column name. Select the columns that you want displayed or hidden by selecting or clearing the items in the list. When you complete the configuration, click **OK**. The columns are displayed in the table as you specified.

Additional functions on this window include:

OK
To perform the operation, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Add Tasks to Task List

Use this action to add one or more tasks to the selected task list. The table contains the list of groupable tasks contained in the role that are not already included in the task list. If the task list already contains all groupable tasks in the role, then the message "No items to display" is shown. You can select all tasks by selecting the top check box.

Use the Filter function to enter a filter string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

You can work with the table by using the table icons or **Actions** list from the table toolbar. If you place your cursor over an icon, the icon description is displayed. the following functions are available from the table toolbar:

Export as HTML
Downloads table data into a Hypertext Markup Language (HTML) file. This action is only available when you are using a remote browser.

Export All to CSV
Downloads table data into a Coma Separated Values (CSV) file. You can then import the downloaded CSV file into most spreadsheet applications. This action is only available when you are using a remote browser.

Print All
Prints all rows in the table. This action is only available when you are using a remote browser.

Print Selected
Prints selected rows in the table. This action is only available when you are using a remote browser.

Print Preview
Displays a printable version of all rows in the table. This action is only available when you are using a remote browser.

Configure Options
Selects the columns that you want to display. All available columns are in the list by their column name. Select the columns that you want displayed or hidden by selecting or clearing the items in the list. When you complete the configuration, click **OK**. The columns are displayed in the table as you specified.

Additional functions on this window include:

OK
To perform the operation and update the Task Lists table, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

User Patterns

This task is used by an access administrator or a user that is assigned a role with Manage User Patterns task permission.

Use the **User Patterns** tasks to define a group of console users at once whose user IDs all match a certain pattern. These user IDs are validated against entries in your LDAP server. When a user logs on, if the user ID is not defined locally, it is matched against all the patterns defined. The order of the pattern definitions in the list controls the order in which they are tried. When a match is found, a temporary user definition is created from the user template named in the pattern definition. The user definition exists only so long as the user is logged on, though any settings they customize will be retained for the amount of time given in the pattern definition. If the user logs on again within that period, they do not need to customize the same settings they did previously.

If preferred, you can use the LDAP groups membership lookup table to configure an LDAP group to template assignment or use a template based on an LDAP attribute. You can name an LDAP attribute whose value is the name of the user template that should be used for that user instead of the one named in the pattern definition. This capability gives certain users different privileges than the default for that pattern. Additionally, you can name an LDAP attribute whose value is the name of the console domain that is allowed to log on using that LDAP entry. LDAP attributes can have multiple values in an LDAP entry, and if this attribute name is specified in the pattern definition, one of the attribute values must match the console's domain name.

The **User Patterns** dashboard view displays a list of all currently defined user patterns with user pattern summary sections as follows:

General
This section contains the name and description for the selected user pattern.

Pattern
This section contains the user pattern, the pattern type, and the user settings retention time for the selected user pattern.

Template
This section contains the user template definition, LDAP group membership lookup, LDAP group to template assignments, default template option, and LDAP attribute lookup.

User Access
This section contains user ID log in access based on LDAP attribute, LDAP server, and domain name restriction attribute.

You can view the object Summary using the **Expand** or **Collapse** icons to view or hide sections. You can create a new user pattern using the **New User Pattern** wizard or manage an existing user pattern definition with **User Pattern Details**.

- Click the **"New User Pattern" on page 907** () icon to create a new user pattern. When the **New User Pattern** wizard completes, the new user pattern is added to the User Patterns list.

- Click the **"User Pattern Details" on page 911** () icon to view or modify an existing user pattern.

- Click the **Delete** () icon to delete an existing user pattern. You can delete a pattern that currently has users authenticated using the pattern definition. Use the **Users and Tasks** task to see the list of users currently logged on. You can then forcibly logoff any users that are using the pattern being deleted.
- Click the **Move Up** arrow to move a specific defined user pattern up in the list of defined patterns. You can use this to change the order in which the user patterns are searched.
- Click the **Move Down** arrow to move a specific defined user pattern down in the list of defined patterns. You can use this to change the order in which the user patterns are searched.

New User Pattern

Use the **New User Pattern** wizard to guide you through creating a new user pattern. The **New User Pattern** wizard is organized into the following pages. Each page is listed on the left navigation. The currently displayed page is highlighted.

- Use the "Name" on page 907 page to specify the user pattern name and optional description. It also provides capability to create a new pattern or copy an existing pattern.
- Use the "User Pattern" on page 908 page to define the string pattern to match user IDs.
- Use the "Template Settings" on page 910 page to select the user template to use with this user pattern.
- Use the "User Access" on page 911 page to select which users matching the pattern have log in access to the HMC.
- Use the Summary page to view a summary report of the new user pattern to be created. When you click **Finish**, the new user pattern is created and populated with the values specified in the **New User Pattern** wizard.

The new **User Pattern** wizard displays the Welcome page when you start the task for the first time. This page provides a summary of the steps that you will complete to create your new user pattern. Select **Show this welcome page next time** to clear the box if you do not want to display the Welcome page next time you use the **New User Pattern** wizard.

Additional functions on this window include:

Back
To navigate to the previous page in the wizard, click **Back**.

Next
To navigate to the next page in the wizard, click **Next**.

Finish
To create the new user pattern, click **Finish**.

Cancel
To exit the wizard without creating the new user pattern, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

Name

Use the Name page to enter a name and description for the new user pattern you want to create. After entering the information, click **Next** to proceed to the next page.

Create Option
This option determines how the object is created.

New:
Create a new user pattern

New based on:
Select an existing pattern to base the new user pattern on. The settings in the new user pattern are initialized to those of the existing user pattern.

Pattern Details
This section requires a name and an optional description.

Name:
Specify the name for the new user pattern you are creating or managing. When creating a new user pattern, the name can be 1 to 64 characters in length, cannot begin or end with a space, a combination of upper and lower-case letters (A-Z, a-z), numbers (0-9), and the following special characters:

- period (.)
- hyphen (-)
- at sign (@)
- underscore (_)
- space ( )

The name must be unique among existing user pattern names. The comparison for duplicate name is case insensitive.

Description:
Specify an optional meaningful text for your user pattern. The description can be up to 1024 characters with no character restrictions.

User Pattern

Use the User Pattern page to define the pattern string to use in matching user IDs. Select from glob-like pattern or regular expression. After entering the information, click **Next** to proceed to the next page.

Glob-like
Indicates a particular pattern. An asterisk in the pattern matches zero or more characters in the user ID, and a question mark in the pattern matches any single character in the user ID.

Regular expression
Indicate a specific means for matching strings of patterns; such as, particular characters, words, or patterns of characters.

The following table lists some of the common metacharacter symbols used in a regular expression and gives some examples of how to use them. For a complete description of regular expression rules, you can search the intranet.

Table 6. Common metacharacter symbols

Metacharacter	Match	Regular Expression Example	Example explanation
[]	Any characters inside brackets	*[ab]cd*	Specifies *acd* and *bcd* are valid user IDs.
.	Any single character	*2.29431*	Specifies that any user ID that matching the string has any single character in the between the 2's is valid (for example, *2i29431*).
*****	Match the preceding token zero or more times.	**a.***	Specifies all user IDs of any length starting with 'a' are valid

Table 6. Common metacharacter symbols (continued)

Metacharacter	Match	Regular Expression Example	Example explanation
+	Match the preceding token one or more times.	**a+**	Specifies all user IDs of length one or more, containing all a's, are valid.
.+	One or more occurrences of any character.	**a.+**	Specifies all user IDs of length 2 or more, starting with 'a' are valid.
[^c1-c2]	Any but characters except those in brackets.	*sysprog[^0-9]*	Specifies that the last character of the user ID name cannot have any numbers between 0 and 9 (for example, *0123456789*). The example would allow *sysprogx* but not *sysprog1*.
[c1-c2]	Any range of characters in brackets	*sysprog[A-Z]*	Specifies that the last character of the user ID name must be a capital letter. The example would allow *sysprogA*, *sysprogB*, etc, but not *sysprogx* or *sysprog1*.
?	Makes the preceding token in the regular expression optional	*sysprog1?*	Specifies the '1' is optional at the end of the user ID. The example would allow *sysprog* and *sysprog1*.
|	Matches one expression or the other	*(userone|usertwo)@sampleco.com*	The example would allow *userone@sampleco.com*, *usertwo@sampleco.com*..
\c	Turns off the meaning of any special char '**c**'. The backslash will escape the following special characters allowed in the LDAP user ID **\.?*+()**	*sysprog\+*	Specifies that the last character is a plus sign, not that the user ID can end in one or more backslash's. The example would allow user name *sysprog+*.

User pattern:

Specify the user pattern for the selected pattern type that is matched against the user ID that is entered when the user attempt to log on. This value is required to continue.

Retain user settings

Indicates to retain the settings of users authenticated using this pattern. The values specified in the Retention time (days):

- One or more indicates the number of days to retain.
- Unselected indicates not to retain the settings.
- Default retention time is 90 days.

Template Settings

Use the Template page to define which template is used when a user matches this pattern. Select the radio button that specifies how the pattern's template is identified. After entering the information, click **Next** to proceed to the next page.

Use a specific template
From the table, select the user template that specifies the settings for users matching the pattern. Use the "User Templates" on page 915 dashboard view to create and manage user templates.

Use a template based on user LDAP group membership
Select an LDAP server for a user LDAP group membership lookup, configure LDAP group to template mapping, and choose an optional default template if a user is not found in a group:

LDAP server for user LDAP group lookup
Use the drop-down box to select the LDAP server for a user LDAP group lookup.

LDAP Groups To Template Name Mappings table
Use the LDAP groups membership lookups table to configure an LDAP group to template assignment. If a user is a member of multiple LDAP groups, the template comes from the first group membership match. Click the toolbar icon or **Actions** drop-down to perform the following:

Add
To add an LDAP group for a user ID membership lookup and a template to use when a user ID is found in the group.

Delete
To delete an LDAP group template assignment.

Move Up
To move up an LDAP group template assignment in the table.

Move Down
To move down an LDAP group template assignment in the table.

Optionally, you can select default template or fail login when a template is not found:

Use a default template
Use the drop-down menu to select a default template when a match is not found when checking for a group membership.

Fail login
Select the Fail login when a user is not a member of any of the groups in the group to template mappings, the user cannot login.

Use a template based on an LDAP attribute
Select an LDAP server for the lookup, the attribute which will identify the template to use, and an optional default template to use if the attribute is not found or empty:

LDAP server for attribute lookup:
Use the drop-down menu to select the LDAP server for the LDAP attribute lookup.

Attribute for template name:
Enter the LDAP attribute which will identify the template name.

Select default template or fail login when a template is not found:

Use a default template
Use the drop-down menu to select a default template when a template is not named in the override attribute.

Fail login
Select the Fail login when a user's LDAP directory entry does not contain the override attribute or the attribute is empty.

Add LDAP Group Template Assignment

Use this window to assign a template name to an LDAP group.

LDAP group :
Enter a LDAP group name for the user ID membership lookup

Template name:
Enter a template name to use when a user ID is found in the group.

Additional functions on this window include:

Add
To add an LDAP group name to a New Pattern, click **Add**.

Cancel
To cancel the window without adding a LDAP group name to a New Pattern click **Cancel**.

Help
To display help for the current window, click **Help**.

User Access

Use the User Access tab section to view or modify which user access is used when a user matched this pattern. Select the user access that specifies the settings for users matching the pattern.

All users matching the pattern can log in
Select for log in access to the HMC for users matching a specific pattern.

Specific users matching the pattern can log in
Specify the LDAP server and attribute that whose value defines which HMCs the user can log in:

LDAP server for attribute lookup
Specify the LDAP server name for the attribute lookup.

Domain name restriction attribute
Specify the name of the LDAP attribute that contains the information about what console the user is allowed to log on.

User Pattern Details

Use the **User Pattern Details** task to view and manage the properties of a selected user pattern. Use the navigation links on the left to display each tab or use the **Expand All** and **Collapse All** icons to display each view.

- Select the “General” on page 912 navigation link or the **Expand** icon to display the General details tab section.
- Select the “Pattern” on page 912 navigation link or the **Expand** icon to display the Pattern details tab section.
- Select the “Template” on page 913 navigation link or the **Expand** icon to display the Template details tab section.
- Select the “User Access” on page 915 navigation link or the **Expand** icon to display the User Access details tab section.

Additional functions on this window include:

OK
To save the current changes and exit the task, click **OK**.

Apply
To save the current changes for the user pattern without exiting the task, click **Apply**.

Cancel
To exit the window, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

General

Use the General details tab section to view or modify a user pattern name and description for the selected user pattern.

Name:
Specifies the name for the user pattern you are modifying. When you are modifying the user pattern name, the name can be 1 to 64 characters in length, cannot begin or end with a space, a combination of upper and lower-case letters (A-Z, a-z), numbers (0-9), and the following special characters:

- period (.)
- hyphen (-)
- at sign (@)
- underscore (_)
- space ( )

Description:
Specify an optional meaningful text for your user pattern.

Object ID:
Specifies the associated Universal Unique Identifier (UUID) of the managed object.

Note: This value cannot be modified.

Pattern

Use the Pattern details tab section to view or modify a particular pattern.

Glob-like
Indicates a particular pattern. An asterisk in the pattern matches zero or more characters in the user ID, and a question mark in the pattern matches any single character in the user ID.

Regular expression
Indicate a specific means for matching strings of patterns; such as, particular characters, words, or patterns of characters.

The following table lists some of the common metacharacter symbols used in a regular expression and gives some examples of how to use them. For a complete description of regular expression rules, you can search the intranet.

Table 7. Common metacharacter symbols

Metacharacter	Match	Regular Expression Example	Example explanation
[]	Any characters inside brackets	*[ab]cd*	Specifies *acd* and *bcd* are valid user IDs.
.	Any single character	*2.29431*	Specifies that any user ID that matching the string has any single character in the between the 2's is valid (for example, *2i29431*).
*****	Match the preceding token zero or more times.	**a.***	Specifies all user IDs of any length starting with 'a' are valid
+	Match the preceding token one or more times.	**a+**	Specifies all user IDs of length one or more, containing all a's, are valid.

Table 7. Common metacharacter symbols (continued)

Metacharacter	Match	Regular Expression Example	Example explanation
.+	One or more occurrences of any character.	**a.+**	Specifies all user IDs of length 2 or more, starting with 'a' are valid.
[^c1-c2]	Any but characters except those in brackets.	*sysprog[^0-9]*	Specifies that the last character of the user ID name cannot have any numbers between 0 and 9 (for example, *0123456789*). The example would allow *sysprogx* but not *sysprog1*.
[c1-c2]	Any range of characters in brackets	*sysprog[A-Z]*	Specifies that the last character of the user ID name must be a capital letter. The example would allow *sysprogA*, *sysprogB*, etc, but not *sysprogx* or *sysprog1*.
?	Makes the preceding token in the regular expression optional	*sysprog1?*	Specifies the '1' is optional at the end of the user ID. The example would allow *sysprog* and *sysprog1*.
|	Matches one expression or the other	*(userone|usertwo)@sampleco.com*	The example would allow *userone@sampleco.com*, *usertwo@sampleco.com*.
\c	Turns off the meaning of any special char '**c**'. The backslash will escape the following special characters allowed in the LDAP user ID **\.? *+()**	*sysprog\+*	Specifies that the last character is a plus sign, not that the user ID can end in one or more backslash's. The example would allow user name *sysprog+*.

User pattern:
Specify the user pattern for the selected pattern type that is matched against the user ID that is entered when the user attempt to log on.

Retain user settings
Indicates to retain the settings of users authenticated using this pattern. The values specified in the Retention time (days):

- One or more indicates the number of days to retain.
- Unselected indicates not to retain the settings.

Template

Use the Template details tab section to view or modify which template is used when a user matched this pattern. Select the radio button that specifies how the pattern's template is identified. After entering the information, click **Next** to proceed to the next page.

Use a specific template
From the table, select the user template that specifies the settings for users matching the pattern. Use the "User Templates" on page 915 dashboard view to create and manage user templates.

Use a template based on user LDAP group membership
Select an LDAP server for a user LDAP group membership lookup, configure LDAP group to template mapping, and choose an optional default template if a user is not found in a group:

LDAP server for user LDAP group lookup
Use the drop-down box to select the LDAP server for a user LDAP group lookup.

LDAP Groups To Template Name Mappings table
Use the LDAP groups membership lookups table to configure an LDAP group to template assignment. If a user is a member of multiple LDAP groups, the template comes from the first group membership match. Click the toolbar icon or **Actions** drop-down to perform the following:

Add
To add an LDAP group for a user ID membership lookup and a template to use when a user ID is found in the group.

Delete
To delete an LDAP group template assignment.

Move Up
To move up an LDAP group template assignment in the table.

Move Down
To move down an LDAP group template assignment in the table.

Optionally, you can select default template or fail login when a template is not found:

Use a default template
Use the drop-down menu to select a default template when a match is not found when checking for a group membership.

Fail login
Select the Fail login when a user is not a member of any of the groups in the group to template mappings, the user cannot login.

Use a template based on an LDAP attribute
Select an LDAP server for the lookup, the attribute which will identify the template to use, and an optional default template to use if the attribute is not found or empty:

LDAP server for attribute lookup:
Use the drop-down menu to select the LDAP server for the LDAP attribute lookup.

Attribute for template name:
Enter the LDAP attribute which will identify the template name.

Select the default template or fail login when a template is not found:

Use a default template
Use the drop-down menu to select a default template when a template is not named in the override attribute.

Fail login
Select the Fail login when a user's LDAP directory entry does not contain the override attribute or the attribute is empty.

Add LDAP Group Template Assignment

Use this window to assign a template name to an LDAP group.

LDAP group :
Enter an LDAP group name for the user ID membership lookup

Template name:
Enter a template name to use when a user ID is found in the group.

Additional functions on this window include:

Add
To add an LDAP group assignment to a New Pattern, click **Add**.

Cancel
To cancel the window without adding an LDAP group assignment to a New Pattern click **Cancel**.

Help
To display help for the current window, click **Help**.

User Access

Use the User Access details tab section to view or modify which user access is used when a user matched this pattern. Select the user access that specifies the settings for users matching the pattern..

All users matching the pattern have log in access to the HMC
Select for log in access to the HMC for users matching a specific pattern.

Specific users matching the pattern can log in
Specify the LDAP server and attribute that whose value defines which HMCs the user can log in:

LDAP server for attribute lookup
Specify the LDAP server name for the attribute lookup.

Domain name restriction attribute
Specify the name of the LDAP attribute that contains the information about what console the user is allowed to log on.

User Templates

This task is used by an access administrator or a user that is assigned a role with Manage User Templates task permission.

Use the **User Templates** task to create a *user template* that defines the settings and permission for users authenticated with a user pattern. The user IDs are validated against entries in the LDAP server specified by the template. When a user logs on, if the user ID is not defined locally, it is matched against all the patterns defined. The order of the pattern definitions in the list controls the order in which they are tried. When a match is found, a temporary user definition is created from the user template named in the pattern definition. The user definition exists only so long as the user is logged on, though any settings they customize will be retained for the amount of time given in the pattern definition. If the user logs on again within that period, they do not need to customize the same settings they did previously.

The **User Templates** dashboard view displays a list of all currently defined user templates with template summary sections as follows:

General
This section contains the description and LDAP server for the selected user template.

Roles
This section lists all of the role permissions assigned to the selected user template.

Groups
This section lists all of the user-defined custom groups (including pattern match groups) that the selected user template has Group Management permission to modify. Groups that the user template is granted only Child Management permission are not shown.

Tasks
This section lists all of the tasks the selected user template is granted permission by the assigned roles. The list does not include tasks that the user template has available by “Default Permissions” on page 888.

Object Types
This section lists all object types the selected user template is granted permission by the assigned roles. The list does not include object types that the user template has available by “Default Permissions” on page 888.

Objects
This section lists all the objects the selected user template is granted permission to access by the assigned roles. Permission has been granted in a role by either object type, specific object, or Child Management permission to a group. This does not include objects that the user template has available by "Default Permissions" on page 888.

You can view the object summary using the **Expand** and **Collapse** icons to view or hide sections. You can create a new user template using the **New User Template** wizard or manage an existing user template definition with the **User Template Details** task.

- Click the **"New User Template" on page 916** () icon to create a user template definition. When the **New User Template** wizard completes, the new user template is added to the User Templates list.
- Click the **"User Template Details" on page 918** () icon to view or modify an existing user template.
- Click the **Delete** () icon to delete an existing user template. You cannot delete a user template that is utilized by a user pattern.

New User Template

Use the **New User Template** wizard to guide you through creating a new user template. The **New User Template** wizard is organized into the following pages. Each page is listed on the left navigation. The currently displayed page is highlighted. Use the Filter function to enter a filter string in the Filter input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

- Use the "Name" on page 917 page to specify the user template name and optional description. It also provides capability to create a new template or copy an existing template.
- Use the "Authentication" on page 917 page to select from a list of LDAP servers to use with this user template.
- Use the "Roles" on page 918 page to select one or more roles to define access permissions for the new user template. You can click on the links for the roles to open **Role Details** for that role. If desired, you can make modification to user-defined roles from **Role Details**.
- Use the Summary page to view a summary report of the new user template to be created. When you click **Finish**, the new user template is created and populated with the values specified in the **New User Template** wizard.

The **New User Template** wizard displays the Welcome page when you start the task for the first time. This page provides a summary of the steps that you will complete to create your new user template. This dashboard provides a summary of the steps that you will complete to create your new task permissions. Select **Show this welcome page next time** to clear the box if you do not want to display the Welcome page next time you use the **New User Template** wizard.

Additional functions on this window include:

Back
To navigate to the previous page in the wizard, click **Back**.

Next
To navigate to the next page in the wizard, click **Next**.

Finish
To create the new user template, click **Finish**.

Cancel
To exit the wizard without creating the new user template, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

Name

Use the Name page to enter a name and description for the new user template you want to create. After entering the information, click **Next** to proceed to the next page.

Create Option
This option determines how the object is created

New
Create a new user template

New based on:
Select an existing template to base the new user template on

User Details
This option requires a name and an optional description.

Name
Specify the user name for the user profile you are creating. When creating a new user template , the user ID can be 4 to 320 characters in length and a combination of upper and lower-case letters (A-Z, a-z), numbers (0-9), and the following special characters:

- back slash (\)
- greater than (>)
- less than (<)
- asterisk (*)
- ampersand (&)
- question mark (?)
- apostrophe (')
- quotation mark (")
- comma (,)
- colon (:)
- left and right parentheses ( )
- semicolon (;)
- number sign (#)
- percent sign (%)
- equals sign (=)
- plus sign (+)
- dash (-)
- underscore (_)
- at sign (@)
- slash (/)
- period (.)

Description
Specify an optional meaningful message for your records.

Authentication

Use the Authentication page to select the LDAP server and the MFA type to use with this new user template. Use the Filter function to enter a filter string in the input field or click the **Advanced Filter** icon to define a filter for any columns that limits the entries in a table.

- **Multi-factor authentication (MFA)**:
  - Select **No MFA**, if users defined by this template are not required to use multi-factor authentication when logging on to the console.

– Select **SE MFA** to require users defined by this template to use the console's TOTP authentication when logging on to the console.

Roles

Use the Roles page to select new role permissions for the new user template. Use the Filter function to enter a filter string in the input field or click the **Advanced Filter** icon to define a filter for any columns that limits the entries in a table.

You can click on the links for the roles to open **Role Details** for that role. If desired, you can make modifications to user-defined roles from **Role Details**. Additional functions on this window include:

OK
To perform the operation and save the changes to user template, click **OK**.

Apply
To save the current changes without exiting the task, click **Apply**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

User Template Details

Use the **User Template Details** task to view and manage the properties of a selected user template. Use the navigation links on the left display each tab or use the **Expand All** and **Collapse All** icons to display each view.

- Select the "General" on page 918 navigation link or the **Expand** icon to display the General details tab section.
- Select the "Session" on page 919 navigation link or the **Expand** icon to display the Session details tab section.
- Select the "Authentication" on page 920 navigation link or the **Expand** icon to display the Authentication details tab section.
- Select the **Roles** navigation link or the **Expand** icon to display the Roles details tab section. Use the **Actions** drop-down to "Add Roles" on page 920 or Remove Roles defining access permission for the user template. You can click on the links for the roles to open **Role Details** for that role. If desired, you can make modifications to user-defined roles from **Role Details**.

Additional functions on this window include:

OK
To save the current changes and exit the task, click **OK**.

Apply
To save the current changes for the user template without exiting the task, click **Apply**.

Cancel
To exit the window, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

General

Use the General tab view to

Name
Specify the user name for the user template you are modifying. When modifying user template, the user ID can be 4 to 320 characters in length and a combination of upper and lower-case letters (A-Z, a-z), numbers (0-9), and the following special characters:

- back slash (\)

- greater than (>)
- less than (<)
- asterisk (*)
- ampersand (&)
- question mark (?)
- apostrophe (')
- quotation mark (")
- comma (,)
- colon (:)
- left and right parentheses ( )
- semicolon (;)
- number sign (#)
- percent sign (%)
- equals sign (=)
- plus sign (+)
- dash (-)
- underscore (_)
- at sign (@)
- slash (/)
- period (.)

Description
Specify an optional meaningful message for your records.

Session

Use the Session details tab section to view or modify the interval, in minutes, that the user session can run before being prompted for identity verification.

Note: If you use the **Single Object Operations** task from the Hardware Management Console, the session timeout is disabled on the Support Element for the duration of the Single Object Operations session.

Session timeout (minutes):
Select this to specify the interval, in minutes, over which a user's session can run before being prompted for identity verification. If a value other than zero is specified, the user is prompted after the specified minutes have been reached to re-enter their password. If a password is not re-entered within the amount of time that was specified in the *Verify timeout minutes* field, then the session is disconnected. You can specify up to a maximum value of 525600 minutes (equivalent to one year). There is no expiration when unselected.

Verify timeout (minutes):
Select this to specify the amount of time that is required for the user to re-enter their password when prompted, if a value was specified in the *Session timeout minutes* field. If the password is not re-entered within the specified time, the session will be disconnected. The default is 15 minutes. You can specify up to a maximum value of 525600 minutes (equivalent to one year). There is no expiration when unselected.

Idle timeout (minutes):
Select this to specify the number of minutes the user's session can be idle. If the user does not interact with the session in the specified amount of time, the session will be disconnected. You can specify up to a maximum value of 525600 minutes (equivalent to one year). There is no expiration when unselected.

Authentication

Use the Authentication details tab section to view or modify the LDAP server selected to be used for authentication.

- Use **Enterprise Directory Server (LDAP)** to modify the LDAP server selected for the user template. Click the drop-down for the list of servers, then select one.
- Select **Delay login after failed attempts** to enable the logon delay for continual invalid login attempts.

  Number of failed attempts before disable delay
  Specify the number of failed attempts before the user is temporarily disabled from being able to log on.

  Delay (minutes)
  Specify the amount of time in minutes the user is temporarily disabled after reaching the number of failed attempts.
- Select **Disable for inactivity (days):** to specify that a user is disabled if they have not logged on within a specified number of days. Then, specify the number of days after which the inactive user becomes disabled.
- Select **Require password for disruptive actions** to enable a password requirement, for this user template, on a task that causes disruptive actions. This option, by default, is selected.
- Select **Require text input for disruptive actions** to enable a text input requirement before performing a disruptive action on an object.
- **Multi-factor authentication (MFA)**:
  - Select **No MFA**, if users defined by this template are not required to use multi-factor authentication when logging on to the console.
  - Select **SE MFA** to require users defined by this template to use the console's TOTP authentication when logging on to the console.
  - To require this template receive a new shared secret key the next time the user logs on to the console, click **Reset**. This option is only available when you select **SE MFA**.

Default Group

Use the Default group field to choose the default group for the user. A *default group* is a user-defined group to which objects created by the user will be added by default. Use the drop-down to choose either **No default group** or select the desired group.

Default group
Choose a group that objects created by the user are added by default. The administrator should ensure that the user has access permission to manage the default group. Select **No default group** if you do not want to have new objects created by the user added to a group.

The default group cannot be a pattern match group since new objects defined by the user might not match the specific pattern for the group. Thus, no pattern match groups are included in the list.

Tasks that result in objects being added to a default group are as follows:

- Grouping

Add Roles

Use this action to select new role permissions for the user template. Use the Filter function to enter a filter string in the input field or click the **Filter** icon to define a filter for any columns that limits the entries in a table.

You can click on the links for the roles to open **Role Details** for that role. If desired, you can make modifications to user-defined roles from **Role Details**.

Additional functions on this window include:

OK
To perform the operation and save the changes to user template, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Password Rules

This task is used by an access administrator or a user that is assigned a role with Manage Password Rules task permission. Use this task to create, customize, or verify the password rules assigned to the system users.

Password rules assign individual rules for the system user when they are creating a password. In addition, you can optionally set more specific rules for individual parts of the password by specifying one or more character rules. There are three default password rules that you can choose from if you do not want to create your own. They are Basic, Strict, and Standard.

The **Password Rules** dashboard view displays a list of all currently defined password rules and password rule summary sections as follows:

General
This section contains the description for the selected password rule.

Password Rules
This section contains the expiration, minimum and maximum character length of password, consecutive number of characters allowed to be repeated in a row, similarity count, history count, and case sensitive settings for the selected password rule.

Character Rules
This section contains a table of the character rules for the selected password rule. The table specifies the minimum length, maximum length, alphabetic, numeric, special, and user-defined custom character specifications for the character rule parts.

You can view the object summary using the **Expand** and **Collapse** icons to view or hide sections. You can create a new password rule using the **New Password Rule** wizard or manage an existing password rule definition with **Password Rules Details**.

- Click the **"New Password Rule" on page 921**() icon to create a new password rule. When the **New Password Rule** wizard completes, the password rule is added to the Password Rules list.
- Click the **"Password Rule Details" on page 924**() icon to view or modify an existing password rule. You cannot modify the system defined password rules: Basic, Standard, and Strict.
- Click the **Delete** () icon to delete an existing password rule. You cannot delete a password rule that is utilized by at least one user.

New Password Rule

Use the **New Password Rule** wizard to guide you through creating a new case sensitive password rule. The **New Password Rule** wizard is organized into the following pages. Each page is listed on the left navigation. The currently displayed page is highlighted.

- Use the "Name" on page 922 page to specify the password rule name and optional description. It also provides capability to create a new password rule or copy an existing password rule.
- Use the "Password Rules" on page 923 page to define settings and restrictions for the new password rule.

- Use the “Character Rules” on page 923 page to create rules which define character restrictions for the sections of the password.
- Use the Summary page to view a summary report of the new password rule to be created. When you click **Finish**, the new password rule is created and populated with the values specified in the **New Password Rule** wizard.

The **New Password Rule** wizard displays the Welcome page when you start the task for the first time. This page provides a summary of the steps that you will complete to create your new password rule. Select **Show this welcome page next time** to clear the box if you do not want to display the Welcome page next time you use the **New Password Rule** wizard.

Additional functions on this window include:

Back
To navigate to the previous page in the wizard, click **Back**.

Next
To navigate to the next page in the wizard, click **Next**.

Finish
To create the new password rule, click **Finish**.

Cancel
To exit the wizard without creating the new password rule, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

Name

Use the Name page to enter a name and description for the new password rule you want to create. After entering the information, click **Next** to proceed to the next page.

Create Option
This option determines how the object is created.

New:
Create a new password rule.

New based on:
Select an existing password rule to base the new password rule on. The settings in the new password rule are initialized to those of the existing password rule.

Password Rule Details
This section requires a name and an optional description.

Name:
Specify the name for the new password rule you are creating. When creating a new password rule, the name can be 1 to 64 characters in length, cannot begin or end with a space, a combination of upper and lower-case letters (A-Z, a-z), numbers (0-9), and the following special characters:

- period (.)
- hyphen (-)
- at sign (@)
- underscore (_)
- space ( )

The name must be unique among existing password rule names. The comparison for duplicate name is case insensitive.

Description:
Specify an optional meaningful text for your password rule. The description can be up to 1024 characters with no character restrictions.

Password Rules

Use the Password Rules page to specify the properties for the new password rule. After entering the information, click **Next** to proceed to the next page.

Password never expires
Select whether this password should expire after a set number of days or never expire.

Minimum length
Enter the minimum length of characters you are allowing for this part of the password.

Maximum length
Enter the maximum length of characters you are allowing for this part of the password.

Consecutive characters
Enter the number of times a character can be repeated consecutively. Zero means not set.

History count
Enter the number of previous passwords that are saved before a password can be reused.

Character Rules

Use the Character Rules page to specify the properties for the parts that you want to define for the password rule. A *character rule* sets specific rules for an individual part of the password. Use the **Actions** list to add additional rule parts, edit existing rule parts, remove a rule part for this password rule, or move a rule part up or down in the list of rule parts. After entering the information, click **Next** to proceed to the next page.

Minimum length
The minimum length of characters you are allowing for this part of the password. This value cannot be less than one.

Maximum length
The maximum length of characters you are allowing for this part of the password. This value cannot be less than one. The maximum must be greater than or equal to the minimum number of characters.

Alphabetic characters
Whether you Allowed, Not allowed, or Required use of an alphabetic character in the defined property. Use the drop-down arrow to make your selection.

Numeric characters
Whether you Allowed, Not allowed, or Required use of a numeric character in the defined property. Use the drop-down arrow to make your selection.

Special characters
Whether you Allowed, Not allowed, or Required use of a special character in the defined property. Use the drop-down arrow to make your selection.

Special characters include: greater than (>), less than (<), tilde (~), exclamation mark (!), at sign (@), number sign (#), question mark (?), dollar sign ($), vertical bar (|), percent sign (%), caret (^), ampersand (&), asterisk (*), left and right parentheses ( ), underscore (_), plus sign (+), hyphen (-), equals sign (=), left and right curly braces ({ }), left and right square brackets ([ ]), back slash (\), forward slash (/), period (.), comma (,), colon (:), accent (`), quotation mark ("), semicolon (;), and apostrophe (').

Custom Character Set 1
Specifies a user-defined character set for this rule.

Custom Character Set 2
Specifies a second user-defined character set for this rule.

Add/Edit Character Rules

Use this action to add or edit the character rules for this fragment of the password. A *character rule* sets specific rules for an individual part of the password.

Minimum length
The minimum length of characters you are allowing for this part of the password. This value cannot be less than one.

Maximum length
The maximum length of characters you are allowing for this part of the password. This value cannot be less than one. The maximum must be greater than or equal to the minimum number of characters.

Alphabetic characters
Whether you Allowed, Not allowed, or Required use of an alphabetic character in the defined property. Use the drop-down arrow to make your selection.

Numeric characters
Whether you Allowed, Not allowed, or Required use of a numeric character in the defined property. Use the drop-down arrow to make your selection.

Special characters
Whether you Allowed, Not allowed, or Required use of a special character in the defined property. Use the drop-down arrow to make your selection.

Special characters include: greater than (>), less than (<), tilde (~), exclamation mark (!), at sign (@), number sign (#), question mark (?), dollar sign ($), vertical bar (|), percent sign (%), caret (^), ampersand (&), asterisk (*), left and right parentheses ( ), underscore (_), plus sign (+), hyphen (-), equals sign (=), left and right curly braces ({ }), left and right square brackets ([ ]), back slash (\), forward slash (/), period (.), comma (,), colon (:), accent (`), quotation mark ("), semicolon (;), and apostrophe (').

Custom Character Set 1
Specifies a user-defined character set for this rule.

Custom Character Set 2
Specifies a second user-defined character set for this rule.

Additional functions on this window include:

OK
To perform the operation, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Password Rule Details

Use the **Password Rule Details** task to view and manage the properties of a password rule. You cannot modify the system defined password rules (Basic, Standard, and Strict). Use the navigation links on the left to display each tab or use the **Expand All** and **Collapse All** icons to display each view.

- Select the "General" on page 925 navigation link or the **Expand** icon to display the General details tab section.
- Select the "Password Rules" on page 925 navigation link or the **Expand** icon to display the Password Rule details tab section.
- Select the "Character Rules" on page 925 navigation link or the **Expand** icon to display the Character Rule details tab section.

Additional functions on this window include:

OK
To save the current changes and exit the task, click **OK**. This function is available only for user-defined password rules.

Apply
To save the current changes for the role without exiting the task, click **Apply**. This function is available only for user-defined password rules.

Close
To exit the window, click **Close**. This function is available only for system defined password rules since they cannot be modified.

Cancel
To exit the window, click **Cancel**. A confirmation window is displayed. The information you entered is not saved. This function is available only for user-defined password rules.

Help
To display help for the current window, click **Help**.

General

Use the General details tab section to modify a description of a password rule.

Name:
Specifies the name for the password rule you are modifying.

Description:
Specify an optional meaningful text for your password rule.

Object ID:
Specifies the associated Universal Unique Identifier (UUID) of the managed object.

Note: This value cannot be modified.

Password Rules

Use the Password Rules details tab section to specify the settings and restrictions to which the password must adhere. After entering the information, click **Next** to proceed to the next page.

Note: You cannot change the rule data for the Basic, Strict, and Standard password rules.

Password never expires
Select whether this password should expire after a set number of days or never expire.

Minimum length
Enter the minimum length of characters you are allowing for this part of the password.

Maximum length
Enter the maximum length of characters you are allowing for this part of the password.

Consecutive characters
Enter the number of times a character can be repeated consecutively. Zero means not set.

History count
Enter the number of previous passwords that are saved before a password can be reused.

Case sensitive
Specifies whether or not the password should be treated in a case sensitive manner. By default, this setting is selected.

Character Rules

Use the Character Rules details tab section to specify the properties for the parts that you want to define for the password rule. A *character rule* sets specific rules for an individual part of the password. Use the **Actions** list to add additional rule parts, edit existing rule parts, remove a rule part for this password rule, or move a rule part up or down in the list of rule parts. After entering the information, click **Next** to proceed to the next page.

Minimum length
The minimum length of characters you are allowing for this part of the password. This value cannot be less than one.

Maximum length
The maximum length of characters you are allowing for this part of the password. This value cannot be less than one. The maximum must be greater than or equal to the minimum number of characters.

Alphabetic characters
Whether you Allowed, Not allowed, or Required use of an alphabetic character in the defined property. Use the drop-down arrow to make your selection.

Numeric characters
Whether you Allowed, Not allowed, or Required use of a numeric character in the defined property. Use the drop-down arrow to make your selection.

Special characters
Whether you Allowed, Not allowed, or Required use of a special character in the defined property. Use the drop-down arrow to make your selection.

Special characters include: greater than (>), less than (<), tilde (~), exclamation mark (!), at sign (@), number sign (#), question mark (?), dollar sign ($), vertical bar (|), percent sign (%), caret (^), ampersand (&), asterisk (*), left and right parentheses ( ), underscore (_), plus sign (+), hyphen (-), equals sign (=), left and right curly braces ({ }), left and right square brackets ([ ]), back slash (\), forward slash (/), period (.), comma (,), colon (:), accent (`), quotation mark ("), semicolon (;), and apostrophe (').

Custom Character Set 1
Displays a user-defined character set for this rule.

Custom Character Set 2
Displays a second user-defined character set for this rule.

Add/Edit Character Rules

Use this action to add or edit the character rules for this fragment of the password. A *character rule* sets specific rules for an individual part of the password.

Minimum length
The minimum length of characters you are allowing for this part of the password. This value cannot be less than one.

Maximum length
The maximum length of characters you are allowing for this part of the password. This value cannot be less than one. The maximum must be greater than or equal to the minimum number of characters.

Alphabetic characters
Whether you Allowed, Not allowed, or Required use of an alphabetic character in the defined property. Use the drop-down arrow to make your selection.

Numeric characters
Whether you Allowed, Not allowed, or Required use of a numeric character in the defined property. Use the drop-down arrow to make your selection.

Special characters
Whether you Allowed, Not allowed, or Required use of a special character in the defined property. Use the drop-down arrow to make your selection.

Special characters include: greater than (>), less than (<), tilde (~), exclamation mark (!), at sign (@), number sign (#), question mark (?), dollar sign ($), vertical bar (|), percent sign (%), caret (^), ampersand (&), asterisk (*), left and right parentheses ( ), underscore (_), plus sign (+), hyphen (-), equals sign (=), left and right curly braces ({ }), left and right square brackets ([ ]), back slash (\), forward slash (/), period (.), comma (,), colon (:), accent (`), quotation mark ("), semicolon (;), and apostrophe (').

Custom Character Set 1
Specifies a user-defined character set for this rule.

Custom Character Set 2
Specifies a second user-defined character set for this rule.

Additional functions on this window include:

OK
To perform the operation, click **OK**.

Cancel
To exit the current window without saving changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

LDAP Server Definitions

This task is used by an access administrator or a user that is assigned a role with Manage LDAP Server Definitions task permission. Use this task to create a new LDAP server definition or you can edit or remove an existing LDAP server definition. The Lightweight Directory Access Protocol (LDAP) support gives you the option to configure your console to use an LDAP server to perform user ID and password authentications at logon time. An LDAP server maintains a tree-structured database serving as a convenient place to put hierarchical information, such as a corporate employee directory. Each level of the LDAP tree generally represents a different type of information. An LDAP server can also be used for group lookups and membership checks depending on how the User Patterns are set up.

The **LDAP Server Definitions** dashboard view displays a list of all currently defined LDAP server definitions with LDAP server definition summary sections as follows:

General
This section contains the description for the selected LDAP server definition.

Host Connection Information
This section contains the primary host name, backup host name, connection port, Secure Sockets Layer (SSL) connection, allow self-signed or untrusted server certificates descriptions.

Initial Bind information
This section contains the Distinguished Name (DN) to bind with and is used to perform the search.

Directory Entry Location
This section specifies the method and details on how to locate a user's directory entry.

You can view the object summary using the **Expand** or **Collapse** icons to view or hide sections. You can create a LDAP server definition using the **New LDAP Server Definition** wizard or manage an existing LDAP server definition with **LDAP Server Definition Details**.

- Click **"New LDAP Server Definition" on page 927**() to create a new LDAP server definition. When the new **LDAP Server Definition** wizard completes, the new LDAP server definition is added to the LDAP Server Definitions list.

- Click **"LDAP Server Definition Details" on page 930**() to view or modify an existing LDAP server definition.

- Click **Delete** () to delete an existing LDAP server definition. You cannot delete an LDAP server definition that is being utilized by at least one user or user template.

New LDAP Server Definition

Use the **New LDAP Server Definition** wizard to guide you through creating a new LDAP server definition. The **New LDAP Server Definition** wizard is organized into the following pages. Each page is listed on the left navigation. The currently displayed page is highlighted.

- Use the "Name" on page 928 page to specify the LDAP server definition name and optional description. It also provides capability to create a new LDAP server definition or copy an existing LDAP server definition.
- Use the "Host Connection" on page 929 page to set host connection information.

- Use the “Bind Information” on page 929 page to optionally add users directory entry credentials.
- Use the “Directory Location” on page 929 page to specify directory entry location settings.
- Use the Summary page to view a summary report of the new LDAP server definition to be created. When you click **Finish**, the new LDAP server definition is created and populated with the values specified in the **New LDAP Server Definition** wizard.

The New **LDAP Server Definition** wizard displays the Welcome page when you start the task for the first time. This page provides a summary of the steps that you will complete to create your new LDAP server definition. Select **Show this welcome page next time** to clear the box if you do not want to display the Welcome page next time you use the **New LDAP Server Definition** wizard.

Additional functions on this window include:

Back
To navigate to the previous page in the wizard, click **Back**.

Next
To navigate to the next page in the wizard, click **Next**.

Finish
To create the new LDAP server definition, click **Finish**.

Cancel
To exit the wizard without creating the new LDAP server definition, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

Name

Use the Name page to enter a name and description for the new LDAP server definition. After entering the information, click **Next** to proceed to the next page.

Create Option
This option determines how the object is created.

New:
Create a new LDAP server definition

New based on:
Select an existing LDAP server definition to base the new LDAP server definition on. The settings in the new LDAP server definition are initialized to those of the existing LDAP server definition.

LDAP Server Definition Details
This section requires a name and an optional description.

Name:
Specify the name for the user you are creating or managing. When creating a new LDAP server definition, the name can be 1 to 64 characters in length, cannot begin or end with a space, a combination of upper and lower-case letters (A-Z, a-z), numbers (0-9), and the following special characters:

- period (.)
- hyphen (-)
- at sign (@)
- underscore (_)
- space ( )

The name must be unique among existing LDAP server definition names. The comparison for duplicate name is case insensitive.

Description:
Specify an optional meaningful text for your LDAP server definition. The description can be up to 1024 characters with no character restrictions.

Host Connection

Use the Host Connection page to add the host connection name for the LDAP server definition. After entering the information, click **Next** to proceed to the next page.

Primary host name:
Specify the host name or IP address of the computer running the enterprise directory server.

Backup host name:
Specify the host name or IP address of the computer running a backup enterprise directory server. This field is optional, but if specified, this server is accessed if the primary server is not accessible. The LDAP directory hosted by this server is expected to be a mirror of the primary server, allowing the same entry lookup criteria to be used.

Connection port:
Specify the TCP port on which the server accepts connections. If a port is not specified, the default port is used: 389 for a non-secure connection, 636 for a secure connection. 636 is used if you selected **Use a Secure Sockets Layer (SSL) connection**.

Use a Secure Sockets Layer (SSL) connection
Select if you want the console to use a secure socket connection when connecting to the LDAP server. This requires that the LDAP server and the console support a common SSL or TLS version (see the **Customize Console Services** task) and that they also support a common cipher suite.

Allow self-signed or untrusted server certificates
If you selected to use a secure sockets layer connection, then option to allow self signed or untrusted server certificates is available. Selecting this option suppresses the error that would otherwise be recognized when the server returns its certificate to the authentication client and that certificate is found to be signed by an unrecognized Certificate Authority. If the server's certificate is signed by a corporate signing certificate, then another option is to import that signing certificate using the **Certificate Management** task. After the import, the server's certificate chain can be verified.

Bind Information

Use the Bind Information page to optionally add the distinguished name (DN) and password for the new LDAP server definition. After entering the information, click **Next** to proceed to the next page.

Distinguished Name (DN):
Specify a distinguished name to bind with for initial connection. This DN is used to perform the search. If no connection name is specified, the initial connection is anonymous. The fully-qualified name of an entry is called the *distinguished name (DN)*. It is formed by starting with the name of the entry and appending the name of the nodes encountered when going from that entry to the root of the tree, separated by commas.

For example: "cn=Tom Smith, loc=New York, ou=ABC, o=xyz.com"

Password:
Specify a password to bind with on the initial connection. This is only required when a bind name is specified.

Confirm password:
Re-specify the password that you previously entered.

Directory Location

Use the Directory Location page to set a distinguished name pattern or search tree. After entering the information, click **Next** to proceed to the next page.

Use DN pattern:
Specify the distinguished name pattern in the input field. The DN pattern must include the characters `{0}`, indicating where in the pattern the user ID should be substituted. The user ID will be either the name of the user on the console, or, if provided, the string entered into the **LDAP User ID** field of the user definition.

Search DN tree:
Specify the distinguished name in the input field to find a user's directory entry or determine a user's group membership by searching the distinguished name tree, then select one of the following search scope options:

- Select **Entire tree** to search the entire subtree under the base distinguished name entry.
- Select **One level** to search only one level under the base distinguished name entry.

If this LDAP Server Definition is for finding a user, specify an LDAP **Search filter** that selects the user's entry in the directory. This usually matches an attribute in the entry against the user ID. The pattern must include the characters `{0}`, indicating where in the pattern the user ID should be substituted. The user ID will be either the name of the user on the console, or, if provided, the string entered into the **LDAP User ID** field of the user definition.

If this LDAP Server Definition is for finding a group entry in the directory and determining if the user is a member of that group, specify an LDAP **Search filter** that selects the group's entry and searches its membership attribute values. The filter must include the characters `{0}` and `{1}`. `{0}` indicates where in the filter the user's DN should be substituted, and `{1}` indicates where in the filter the group's name should be substituted. If the user is a member of a group, the user's DN will match a value of the group's membership attribute. Since there are two conditions to be met in this search, it should contain a logical AND of the two conditions. For example: `(&(uniqueMember={0})(cn={1}))`.

LDAP Server Definition Details

Use the **LDAP Server Definition Details** task to view and modify the properties of a selected LDAP server definition. Use the navigation links on the left to display each tab or use the **Expand All** and **Collapse All** icons to display each view.

- Select the "General" on page 930 navigation link or the **Expand** icon to display the General details tab section.
- Select the "Host Connection" on page 931 navigation link or the **Expand** icon to display the Host Connection details tab section.
- Select the "Bind Information" on page 931 navigation link or the **Expand** icon to display the Bind Information details tab section.
- Select the "Directory Entry Location" on page 931 navigation link or the **Expand** icon to display the Directory Entry Location details tab section.

Additional functions on this window include:

OK
To save the current changes and exit, click **OK**.

Apply
To save the current changes for the LDAP server definition without exiting the task, click **Apply**.

Cancel
To exit the window, click **Cancel**. A confirmation window is displayed. The information you entered is not saved.

Help
To display help for the current window, click **Help**.

General

Use the General details tab section to modify the description for the LDAP server definition.

Name:
Specifies the name for the LDAP server definition you are modifying.

Description:
Specify an optional meaningful text for your LDAP server definition.

Object ID:
Specifies the associated Universal Unique Identifier (UUID) of the managed object.

Note: This value cannot be modified.

Host Connection

Use the Host Connection details tab section to view or modify the host connection name of the LDAP server definition.

Primary host name:
Specify the host name or IP address of the computer running the enterprise directory server.

Backup host name:
Specify the host name or IP address of the computer running a backup enterprise directory server. This field is optional, but if specified, this server is accessed if the primary server is not accessible. The LDAP directory hosted by this server is expected to be a mirror of the primary server, allowing the same entry lookup criteria to be used.

Connection port:
Specify the TCP port on which the server accepts connections. If a port is not specified, the default port is used: 389 for a non-secure connection, 636 for a secure connection. 636 is used if you selected **Use a Secure Sockets Layer (SSL) connection**.

Use a Secure Sockets Layer (SSL) connection
Select if you want the console to use a secure socket connection when connecting to the LDAP server. This requires that the LDAP server and the console support a common SSL or TLS version (see the **Customize Console Services** task) and that they also support a common cipher suite.

Allow self-signed or untrusted server certificates
If you selected to use a secure sockets layer connection, then the option to allow self signed or untrusted server certificates is available. Selecting this option suppresses the error that would otherwise be recognized when the server returns its certificate to the authentication client and that certificate is found to be signed by an unrecognized Certificate Authority. If the server's certificate is signed by a corporate signing certificate, then another option is to import that signing certificate using the **Certificate Management** task. After the import, the server's certificate chain can be verified.

Bind Information

Use the Bind Information details tab section to view or modify the bind information of the LDAP server definition.

Distinguished Name (DN):
Specify a distinguished name to bind with for initial connection. This DN is used to perform the search. If no connection name is specified, the initial connection is anonymous. The fully-qualified name of an entry is called the *distinguished name (DN)*. It is formed by starting with the name of the entry and appending the name of the nodes encountered when going from that entry to the root of the tree, separated by commas.

For example: "cn=Tom Smith, loc=New York, ou=ABC, o=xyz.com"

Password:
Specify a password to bind with on the initial connection. This is only required when a bind name is specified.

Confirm password:
Re-specify the password that you previously entered.

Directory Entry Location

Use the Directory Entry Location details tab section to view or modify the directory entry location of the LDAP server definition.

Use DN pattern:
Specify the distinguished name pattern in the input field. The DN pattern must include the characters "`{0}`", indicating where in the pattern the user ID should be substituted. The user ID will be either the

name of the user on the console, or, if provided, the string entered into the **LDAP User ID** field of the user definition.

Search DN tree:
Specify the distinguished name in the input field to find a user's directory entry or determine a user's group membership by searching the distinguished name tree, then select one of the following search scope options:

- Select **Entire tree** to search the entire subtree under the base distinguished name entry.
- Select **One level** to search only one level under the base distinguished name entry.

If this LDAP Server Definition is for finding a user, specify an LDAP **Search filter** that selects the user's entry in the directory. This usually matches an attribute in the entry against the user ID. The pattern must include the characters "`{0}`", indicating where in the pattern the user ID should be substituted. The user ID will be either the name of the user on the console, or, if provided, the string entered into the **LDAP User ID** field of the user definition.

If this LDAP Server Definition is for finding a group entry in the directory and determining if the user is a member of that group, specify an LDAP **Search filter** that selects the group's entry and searches its membership attribute values. The filter must include the characters `{0}` and `{1}`. `{0}` indicates where in the filter the user's DN should be substituted, and `{1}` indicates where in the filter the group's name should be substituted. If the user is a member of a group, the user's DN will match a value of the group's membership attribute. Since there are two conditions to be met in this search, it should contain a logical AND of the two conditions. For example: `(&(uniqueMember={0})(cn={1}))`.

Multi-Factor Authentication

This task is used by an access administrator, a user ID that is assigned access administrator roles or a user that is assigned a role with multi-factor authentication task permission.

Use this task to enable or disable users and templates for SE multi-factor authentication (SE MFA) and reset shared secret keys for one or more users and templates. You can use the **GUIDANCE** information for assistance.

SE MFA

Use SE MFA to enable or disable users and users defined by templates for SE multi-factor authentication (SE MFA) and reset shared secret keys for one or more users and templates. You can use the **GUIDANCE** information for assistance.

Proceed with "Users and Templates" on page 932 to configure for SE MFA.

Users and Templates

Use this table to enable or disable SE MFA for users and users defined by templates. You can select one or multiple names when enabling or disabling users and templates. You can also sort and search within this table. The table columns represent the following:

Name
Displays the names for all the users and templates. Use the arrow in the heading to sort the names alphabetically. Use the search icon above the table to locate a particular user name or template name.

Type
Displays the type of name (**User** or **Template**). Use the arrows in the heading to group the users or the templates.

SE MFA
Displays a check mark for those users or templates, which have SE MFA enabled. Use the arrows in the heading to group all the users and templates, which are enabled for SE MFA.

As you select one or more users or templates to enable or disable for SE MFA, options appear in an action bar above the table. Also, as you complete an option, a message is displayed above the table indicating the action is complete.

Note: You can select more than one name but the **Type** and SE MFA enablement must be the same for all selected names.

The action bar selection includes:

Enable
To enable SE multi-factor authentication for the selected users and templates, click **Enable**. A check mark is displayed in the SE MFA column when the user or template is enabled for multi-factor authentication.

Disable
To disable SE multi-factor authentication for the selected users and templates, click **Disable**. A check mark is no longer displayed in the SE MFA column when the user or template is disabled for multi-factor authentication.

Reset Shared Secret Key
To have the selected users and templates receive a new shared secret key the next time they logon to the console, click **Reset Shard Secret Key**. This action is only available when all selections are enabled for SE MFA.

Cancel
To return to the table without making any updates to the selection, click **Cancel**.

If multi-factor authentication is enabled for a User Template, then all users who are associated with that User Template through a User Pattern are required to use multi-factor authentication to log on to the console.

As changes are made within this table, success messages or error messages are displayed above the table. When you are done reviewing the messages, click the **x** to close.

User Settings

Accessing the User Settings task

Notes:

- Only a user ID assigned access administrator roles sets the defaults of the Support Element console settings by using the **Console Default User Settings** task.
- Because there are many main users interfaces (one for each logged on user), the Support Element console provides each user the ability to change settings. In other words, if you change confirmation settings or controls, this does not cause that same change for other logged-on users.

This task enables you to customize settings that control how the Support Element console operates. You can choose settings such as: single object selection, show tips, or choose when to display or not display confirmation windows.

User Settings

Use the **User Settings** task to customize settings that control how you want the console to operate for your user ID.

User Settings tabs

Use these tabs to control how you want the console to operate for your user ID.

“Confirmations” on page 416
To customize your preferences for using confirmation windows for a subset of console workplace tasks, select the **Confirmations** tab.

“Controls” on page 417
To select the object controls that you prefer, select the **Controls** tab.

Additional options are available from these pages:

Apply
To save the settings currently displayed on this tab, click **Apply**.

Reset
To discard any changes you made to the settings on this tab, and display again the current settings for this window, click **Reset**. If changes have been saved by clicking **Apply**, you can no longer discard the changes.

Defaults
To return to the preferences on this tab to the settings that are the default for the current user, click **Defaults**.

Note: If you are using this option from the **Console Default User Settings** task, then you are returning to the preferences on this tab to the settings that are the system default for all users.

OK
To save the settings on all tabs, click **OK**.

Cancel
To exit this window without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Confirmations

Use this page to customize preferences for using confirmation windows for a subset of tasks.

The preferences you set for using confirmation windows apply to the following subset of tasks:

- Activate
- Deactivate
- Load
- Start
- Start All Processors
- Stop
- Stop All Processors

You can customize the console for displaying a confirmation window upon starting any of the tasks listed above. A confirmation window identifies the task and, optionally, lists the task's target objects. The console operator must use a confirmation window either to confirm starting the task or to cancel it instead.

Confirmation windows reduce the possibility of inadvertently performing tasks, particularly tasks that may disrupt the operation of the Central Processor Complex (CPC) or its images.

Customize the settings to indicate your preferences, then click **Apply**.

Enabled with object list
To display a confirmation window upon starting any of the tasks listed above and to list the task's target objects, select **Enabled with object list**.

Note: The **Load** task does not support this option.

Enabled without object list
To display a confirmation window upon starting any of the tasks listed above, but without listing the task's target objects, select **Enabled without object list**.

Do not show confirmations
To start the tasks listed above without displaying confirmation windows, select **Do not show confirmations**.

Use 'No' as the default action
To set the confirmation window's default action to 'No' upon starting any of the tasks listed above, select **Use 'No' as the default action**.

- If this is selected (a check mark appears) it indicates the default action for the confirmation window is to cancel the task. That is, the **No** button is preselected on the confirmation window, click **No** to cancel the task.
- If this is not selected (a check mark does not appear) it indicates the default action for the confirmation window is to confirm starting the task. That is, the **Yes** button is preselected on the confirmation window, click **Yes** to confirm starting the task.

Controls

Use this page to select the object controls to use on the console.

Single object selection
To select only one object at a time while working on a task, select **Single object selection**. Otherwise, more than one object can be selected while working on a task.

Accept Console Messenger messages
To allow your console sessions to receive Console Messenger chat and broadcast messages, select **Accept Console Messenger messages**. Otherwise, your sessions will not receive these messages, and other sessions attempting to initiate chats with your session will be told that you have elected not to participate in chats.

Note: This option is not available when the Console Messenger facility is disabled. To enable the Console Messenger facility, go to the **Customize Console Services** task.

Bring Chat Window to foreground on new message
The initial chat message window is always displayed in the foreground to notify you of the incoming chat message.

To have the Console Messenger task continue to bring an open chat message window to the foreground after the initial message is received, select **Bring Chat Window to foreground on new message**.

Note: This option is not available when the Console Messenger facility is disabled. To enable the Console Messenger facility, go to the **Customize Console Services** task.

Display timestamps using
To define the time zone that is used to localize timestamps, for those tasks that use timestamps. Select the drop-down arrow to choose your preference.

Notes:

- This is only available for those tasks that are enabled to respect this timestamp setting.
- From the **User Settings** task, if you change your preference and apply this change, a message appears indicating you must restart your login session before the change appears.

Client Time Zone
To display timestamps localized to the time zone of the client browser, select **Client Time Zone**. If you are on a local session, this is the same as the Console Time Zone.

Console Time Zone
To display timestamps localized to the time zone of the Support Element, select **Console Time Zone**. This is the default. If you are on a local session, this is the same as the Client Time Zone.

UTC Time Zone
To display timestamps localized to the UTC time zone, select **UTC Time Zone**.

Console Default User Settings

Use the **Console Default User Settings** task to set the default settings for operating the console.

Only the ACSADMIN default user ID or a user ID with access administrator roles can access this task.

This task will not affect currently logged on users until they log off then log back on.

Console Default User Settings tabs

Use these tabs to set the defaults for controlling how the console operates for all users.

"Confirmations" on page 416
To set preferences for using confirmation windows for a subset of console workplace tasks, select the **Confirmations** tab.

"Controls" on page 417
To set the object controls, select the **Controls** tab.

Additional options are available from these pages:

Apply
To save the settings currently displayed on this window, click **Apply**.

Reset
To discard any changes you made to the settings on this window, and display again the current settings for this window, click **Reset**.

Defaults
To return to the preferences that are the default for the current user, click **Defaults**.

OK
To save the settings, click **OK**.

Cancel
To exit this window without making any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Users and Tasks

Accessing the Users and Tasks task

This task displays a list of the tasks that are running and the users that are currently logged on to the Support Element console.

To work with the users and tasks:

1. Open the **User and Tasks** task. The Users and Tasks window is displayed.
2.
3. The following information is displayed in the *Users Logged On* portion of the window:
   - An ID number associated with the user that is logged on
   - User ID you are logged in as and the other user IDs that are logged in to the console
   - Time the user ID logged in
   - Number of tasks running
   - User ID access location
   - Information about tasks that are running.

   The following information is displayed in the *Running Tasks* portion of the window:
   - Task ID number associated to the task that is running
   - Name of the task that is running
   - Object names that may be targeted for that task
   - An ID number associated with the user running the task

- Time the task was started.

Notes:

- If you are assigned a user ID with access administrator roles, you can:
  - Logoff or disconnect any user from the session (click **Logoff** or **Disconnect**).
  - Terminate any task from the session (click **Terminate**).
- You can only switch to another task in your own session.
- You can terminate your own session.

4. You can initiate a two-way chat with another user by selecting the user name and clicking **Chat With**. You can also switch to another task that is running in your session by selecting the task and clicking **Switch To**.
5. When you have completed the task, click **Close**.

Users and Tasks

Use this task to display a list of the users that are currently logged on to the console.

User's Logged On
This table displays the following information:

Session Id
Specifies the identification number associated with the user that is logged on to the console.

User Name
Specifies the user identification that is logged on to the console.

Logon Time
Specifies the time the user logged on to the console.

Running Tasks
Specifies the number of tasks currently running for the user.

Access Location
Specifies the location the user is accessing the console from.

Notes
Contains additional and useful information pertaining to the session.

If you are assigned a user ID with Access Administrator roles you can select a user from the list and click **Logoff** or **Disconnect**.

Logoff
If you are assigned a user ID with Access Administrator roles, you can select a user from the list and click **Logoff** to log the user off of the console, otherwise this is not an option.

Disconnect
If you are assigned a user ID with Access Administrator roles, you can select a user from the list and click **Disconnect** to disconnect the user from the console, otherwise this is not an option.

Chat With

To initiate a two-way chat with the user of the selected session, click **Chat With**. The **Console Messenger Chat** window is displayed where you can begin your messaging.

If you make more than one selection from the **Users Logged On** list a separate chat window is displayed for each chat partner.

Note: This option is not available when the Console Messenger facility is disabled. To enable the Console Messenger facility, go to the **Customize Console Services** task and enable the **Console messenger** option.

Running Tasks
This table displays the tasks that are currently running and provides the following information:

Task Id
Specifies a task identification number associated to the task that is running.

Task Name
Specifies the name of the task that is running.

Targets
Specifies (if any) the object name(s) that are targeted for that task.

Session Id
Specifies the identification number associated with the user running the task.

Start Time
Specifies the time the task was started.

Switch To
To switch to another task that is running in your session, select the task from the list, then click **Switch To**.

Terminate
To end a task that is running in your session, select the task from the list, then click **Terminate**. If you are assigned a user ID with Access Administrator roles you can end tasks that are in other sessions.

Close
To end this task, click **Close**.

Help
To display help for the current window, click **Help**.

View Activation Profiles

View Activation Profiles

Use this task to view activation profiles for the central processor complex (CPC) and their images.

There are four types of activation profiles:

- Reset profile displays information to activate a CPC and its images
- Load profile displays information to load a previously activated image with a control program or operating system.
- Image profile displays information to activate an image of a CPC previously activated
- Group profile displays information in specifying the capacity of a group of logical partitions.

The following functions are also available from this window:

Cancel
To close the profile page, click **Cancel**.

Help
To display help for the current window, click **Help**.

You can find more detailed help on the following elements of this window:

Profile Tree

This lists all pages for the current profile and a list of referenced profiles and their pages.

Reset pages

The Reset activation profile, referred to also as a CPC profile, displays the CPC name and each image supported by the CPC.

Make a selection from the Profile Tree to view the Reset Profile pages:

General
Displays the selected reset profile and its purpose, and identifies the Input/Output (I/O) configuration and operating mode established for the CPC by the profile.

Storage
Displays the storage configuration established for the CPC by the profile.

Dynamic
Displays information that controls whether the Input/Output (I/O) configuration established for the CPC activated by the profile.

Options
Displays options and information for enabling or disabling global input/output (I/O) priority queuing and customizing options for error handling and recovery for the CPC activated by the profile.

Fenced
Displays the number of available processors when a book is fenced and the processor assignments.

Partitions
Displays a list of logical partitions activated, and the order in which they were activated, on the CPC activated by the profile.

The window includes a section of image pages for each logical partition listed on the **Partitions** page. The information in each section is used to activate the multiple images supported by the CPC.

General

Displays information that describes the selected profile and its purpose and identifies the Input/Output (I/O) configuration and operating mode established for the Central Processor Complex (CPC) activated by the profile.

Profile name
Displays the name of the reset profile selected.

Description
Displays information that describes the contents or purpose of the profile.

IOCDS table
Identifies the Input/Output Configuration Data Set (IOCDS) used during activation to define the Input/Output (I/O) configuration for the Central Processor Complex (CPC).

The I/O configuration is the set of all I/O devices and channel paths available to the CPC.

Input/Output Configuration Data Set
Displays the data set identifier and name of the IOCDS.

Type
Identifies the operating mode supported by the IOCDS.

Note: Activation will fail if a mismatch exists between an IOCDS and mode.

Allow Dynamic I/O
Indicates whether the IOCDS defines an I/O configuration that supports dynamic changes.

Partitions
This column displays the names of logical partitions supported by the IOCDS.

Mode
Identifies the operating mode established during activation to support the number and type of control programs that can operate on the Central Processor Complex (CPC).

Load delay for power sequencing
Specifies the amount of time delayed between completing power-on reset and performing a load.

Storage

This window displays the storage available for allocating to the CPC's logical partitions. The **Mode** list in **General** of this reset profile identifies the operating mode you selected for activating the CPC.

Installed storage
Displays the CPC's amount of installed storage in megabytes.

Customer storage
Displays the storage amount available for allocating to the Central Processor Complex's (CPC) logical partitions.

Dynamic

This window displays information that controls whether the Input/Output (I/O) configuration established for the Central Processor Complex (CPC) activated by the profile can be dynamically changed.

This window displays the Input/Output (I/O) configuration established for the Central Processor Complex (CPC) activated by the profile.

Indicates activating this profile establishes an I/O definition that can be dynamically changed. That is, dynamic I/O will be enabled. Otherwise, this indicates the I/O definition cannot be changed dynamically. That is, dynamic I/O will not be enabled.

The input/output (I/O) definition is the set of all I/O devices and channel paths available to a central processor complex (CPC). An input/output configuration data set (IOCDS) is used during power-on reset as the source of the I/O definition.

Ordinarily, changing the I/O definition requires performing a power-on reset with a modified or different IOCDS. Dynamically changing the I/O definition does not require a power-on reset.

Dynamically changing the I/O definition requires support from the selected IOCDS and from the Hardware Configuration Definition (HCD) feature of a Multiple Virtual Storage (MVS) operating system.

Options

This window displays options and information that enable or disable the global input/output (I/O) priority queueing and options for error handling and recovery for the Central Processor Complex (CPC) activated by the profile.

Enable global input/output (I/O) priority queuing
Indicates whether global I/O priority is enabled or disabled after initial microcode load (IML).

Global I/O priority queuing allows the operating system to specify a priority to be associated with an I/O request at Start Subchannel time. These values are passed to the I/O subsystem for use when making queuing decisions with multiple requests.

Automatic input/output (I/O) interface reset
Indicates whether the I/O interface is reset automatically when any condition occurs that causes shared control units to hold reserves on their devices

- A machine check places the Central Processor Complex (CPC) in a check stopped state.
- A control program places a logical partition in a non-restartable wait state.

Indicates the I/O interface is reset automatically if any of the listed conditions occurs. Otherwise, this indicates the I/O interface is not reset automatically.

In a multiple CPC environment, several objects, which can be CPCs or logical partition, may share the control units, channel paths, and I/O devices included in their I/O interfaces.

Each condition listed above causes shared control units to hold reserves on their devices for the object affected by the condition. Holding reserves provides the affected object with exclusive use of devices, preventing them from being used by other objects that share the control units.

Resetting the I/O interface releases reserves held by shared control units assigned to an object. Their devices become available to other objects.

System recovery time

Indicates whether there is a limit on the amount of time the Central Processor Complex (CPC) is allowed to spend on error handling and recovery.

Limit system recovery time
If selected, recovery time is limited. Otherwise, there is no limit on the amount of time the CPC is allowed to spend on error handler recovery.

When recovery time is limited, error handling and recovery must complete within the specified time limit, otherwise the CPC is put into a checkstop state.

When there is no time limit, the CPC uses as much time as necessary to handle errors. But this does not imply that all errors will be resolved, regardless of how much time the CPC spends on them.

Note: The limit specified for recovery time also determines the type of recovery that is attempted.

Time limit
If recovery time is limited, displays the amount of time the Central Processor Complex (CPC) allowed to spend on error handling and recovery before it is put into a checkstop state.

Note: This field is applicable only when **Limit system recovery time** is selected. Otherwise, this field is unavailable.

The amount of time determines the type of recovery that is attempted. If recovery time is not limited, then all types of recovery are attempted.

Processor running time

Indicates how processor running time is determined.

Processor running time is the amount of continuous time allowed for logical processors to perform jobs on shared processors. The amount of continuous time is also referred to as a timeslice.

Dynamically determined by the system
Indicates the running time whenever the number of active logical processors changes.

Determined by the user
Indicates the constant running time.

Running time
Indicates the constant amount of running time set for logical processors to perform jobs on shared processors in the **Running time** field.

The running time specified is assigned to all logical processors shared by logical partitions activated without dedicated processing resources. Each logical partition has control of shared processor resources for the specified running time. Control passes to the next logical partition when the running time interval expires.

Display fenced book page
Indicates whether or not to display the fenced page.

Fenced Book

This window displays the available system processors assigned when a hardware problem occurs with one of the system books that caused that book to be fenced or become unavailable for use.

- **Number of available processors for Licensed Internal Code** indicates the number of processors that are available in your system.
- **Number of available processors when a book is fenced** indicates the number of processors that your system can use when one book is fenced from use.
- **Number of available processors when a XX processors book is fenced** XX indicates the number of processors that your system can use when the specified processors book is fenced from use.

Processor assignment controls
Displays the processor assignment option.

Determined by the system
Displays if you selected the system to determine how to assign all available processors when a book is fenced from use in your system.

Determined by the user
Displays if you selected to manually assign the processors to your system when a book is fenced from use.

Processor assignments

Displays the processor assignment when a XX processors book is fenced
The XX indicates the number of processors fenced from use.

Processor type
Displays the physical processor assigned to the logical partitions logical processors

LICCC Definition
Displays the amount of licensed internal code installed in your system

Value Used when Book is Fenced
Indicates how many processors have been assigned to the specified processor types.

Partitions

Displays a list of logical partitions to be activated and the order in which they are activated on the Central Processor Complex (CPC) activated by the profile.

Partition
Displays the names of the logical partitions to activate.

Order
Displays the numeric positions of the logical partitions in the activation order.

For each logical partition to be activated, information for activating it in its corresponding set of image pages displays. To display the image pages for a logical partition, select its pages from the profile tree view on the left side of the window.

Load

This window displays information that controls loading a control program for the logical partition activated by the profile.

Profile name
Specifies the name of the profile currently displayed.

Description
Displays information about the contents or the purpose of the profile.

Device type
Indicates the type of device to perform a load for the logical partition. You would use the SCSI or NVMe option to do a standalone dump to a SCSI device or NVMe adapter.

ECKD
Indicates to perform an IPL on the logical partition from ECKD DASD device type.

SCSI
Indicates to perform an IPL on the logical partition from SCSI device type.

NVMe
Indicates to perform an IPL on the logical partition from NVMe device type.

Tape
Indicates to perform an IPL on the logical partition from Tape device type.

IPL type:
Indicates the type of IPL for the selected ECKD device type to perform for the logical partition.

Channel Command Word (CCW)
Indicates to perform the load on Channel Command Word (CCW).

List-directed
Indicates to perform the load on a list-directed IPL.

If the selected load type is **SCSI**, **NVMe**, or **Tape** this field is unavailable.

Load type:

Indicates the type of load to perform for the logical partition. You would use the **ECKD** or **Tape** option to do a standalone dump and select the **Load a dump program** option.

Load an OS

Indicates to perform an operating system load type on the logical partition.

Load a dump program

Indicates to perform a dump program load type on the logical partition.

Validation:

Enable Secure Boot

Indicates to verify the signature of the load program and distributor's signature match.

Certificates

Indicates the assigned certificates keys to enable a secure boot for the selected logical partition.

If the selected device type is **Tape** or **ECKD** and IPL type **CCW** is selected this field is unavailable.

Options:

Store status

Indicates whether the store status function stores the current values of the processing unit timer, the clock comparator, the program status word, and the contents of the processor registers in their assigned absolute storage locations.

- A check mark indicates performing the store status function before the load.
- An empty check box indicates not performing the store status function before the load.

Clear the main memory before loading

Indicates to clear main memory storage on the logical partition before a load.

If the selected device type is **SCSI** or **NVMe** this field is unavailable.

Load address:

Displays the address of the input/output (I/O) device that provides access to the control program to load. For a SCSI load or NVMe load, this field has the device number of the device (for example, fibre channel adapter) that is used to perform the SCSI or NVMe load. This should contain four hexadecimal digits for NVMe load or five hexadecimal digits for SCSI load.

A load address is required.

The source of the control program must be an I/O device in the I/O configuration that is active when this profile is activated. The I/O device can store the control program or can be used to read the control program from a data storage medium.

Note: This field is applicable only when **Use dynamically changed address** check box is empty. Otherwise, if the check box displays a check mark, this field is unavailable.

Use dynamically changed address

Indicates whether the load address is dynamically determined by changes to the channel subsystem Input/Output definition (I/O).

If this is selected, the load address is dynamically determined. Otherwise, this profile sets the load address. See the **Load address** field for the address set by this profile.

Load parameter:

Indicates the optional information, if any, to use to further control how the control program is loaded during activation.

Some control programs support the use of a load parameter to provide additional control over the performance or outcome of a load. Check the configuration programming and reference documentation for the control program to determine the load parameters that are available and their effects on a load.

Note: This field is applicable only when **Use dynamically changed parameter** is **not** selected. Otherwise, this field is unavailable.

Use dynamically changed parameter

Indicates whether the load parameter is dynamically determined by changes to the channel subsystem Input/Output (I/O) definition.

If this is selected, the load parameter is dynamically determined. Otherwise, this profile sets the load parameter. Enter the parameter for this profile in the **Load parameter** field.

Time-out value:

Indicates the amount of time to allow for the completion of the load.

If the load operation cannot be completed within the specified time, the operation is canceled.

If the selected device type is **SCSI**, **NVMe**, or **ECKD** and IPL type **List-directed** is selected, this field is unavailable.

Boot record location:

Indicates the boot record location for an ECKD DASD.

- The **use volume label**specifies the boot record label from the volume label
- Specified the C,H,R format. The Cylinder number is a 4-byte value ranging from '0x00000000' to '0x0FFFFFFF'. The Head number is a 1-byte value ranging from '0x00' to '0x0F'. The Record number is a 1-byte value ranging from '0x01' to '0xFF'.

If the selected device type is **SCSI**, **NVMe**, **Tape**, or **ECKD** and IPL type **CCW** is selected, this field is unavailable.

Worldwide port name:

Displays the Worldwide Port Number identifying the Fibre Channel port of the SCSI target device (according to the FCP/SCSI-3 specifications). This is a 64-bit binary number designating the port name, represented by 16 hexadecimal digits. This is required for SCSI load or SCSI dump.

If the selected device type is **ECKD**, **NVMe** or **Tape**, this field is unavailable.

Logical unit number:

Displays the number of the logical unit as defined by FCP (according to the FCP/SCSI-3 specifications). This is the 64-bit binary number designating the unit number of the FCP I/O device, represented by 16 hexadecimal digits. This field is required for SCSI load or SCSI dump.

If the selected device type is **ECKD**, **NVMe**, or **Tape**, this field is unavailable.

Boot program selector:

Displays the program to load from the FCP-load device and contains a decimal value in the range from 0 to 30.

If the selected device type is **Tape** or **ECKD** and IPL type **CCW** is selected, this field is unavailable.

Boot record logical block address:

Displays the load block address if your file system supports dual-boot or booting from one of the multiple partitions. If no block address is specified, the logical-block address of the boot record is assumed to be zero. This feature could be used to IPL using a second or backup boot record, in case the original one is corrupted or overwritten by accident.

This field is unavailable if a device type of **ECKD** or **Tape** are selected.

Operating system load parameters:

Displays a variable number of characters to be used by the program that is loaded. This information will be given to the IPLed operating system and will be ignored by the machine loader. The IPLed operating system (or standalone dump program) has to support this feature. Any line breaks you enter are transformed into spaces before being saved.

If the selected device type is **Tape** or **ECKD** and IPL type **CCW** is selected, this field is unavailable.

Image pages

This window displays an activation profile for activating a logical partition as an image. The window displays the image name.

Make a selection from the Profile Tree to view the image pages in the profile:

General
Displays the image profile and its purpose, and identifies the operating mode established for the logical partition activated by the profile.

Processor
Displays information that assigns logical processors to the logical partition activated by the profile.

Security
Displays settings that determine the extent of interaction between the logical partition activated by the profile and other logical partitions activated on the CPC.

Storage
Displays the amount of storage assigned to the logical partition activated by the profile.

Options
Displays the image option for the processor values.

Load
Displays information that controls loading a control program for the logical partition activated by the profile.

Note: Not available when Coupling facility or Secure Service Container are selected on the **General** image page.

"SSC" on page 954
Displays the image options for the selected SSC partition.

Crypto
Displays information that controls how the logical partition activated by the profile uses the coprocessors and accelerators assigned to it.

Note: Not available when Coupling facility is selected on the **General** image page.

Time Offset
Displays the logical partition's clock using an offset from the External Time Source's time of day.

Note: Available when **Logical partition offset** is selected on the **General** image page.

General

Displays information on the image profile and its purpose and identifies the operating mode established for the logical partition activated by the profile.

Profile name
Specifies the name of the profile currently displayed.

Description
Displays additional information about the profile, such as the contents or purpose of the profile.

Note: A description is recommended, but optional is and optional profile parameter; some profiles may not have one. The person who customizes the profile provides or omits its description.

Partition identifier
Displays the number of the partition (in hexadecimal). This is used by the program that is operating in the logical partition.

The partition identifier must also be unique among the identifiers of other logical partitions activated by this profile. If necessary, check the partition identifier fields on the other **General** image pages to verify the partition identifier assigned to this image is unique.

Mode
Displays the operating mode established during activation to support the type of control program that can operate on the logical partition.

The mode determines some of the other types of information included in the image profile. Different profile information is associated with each different mode.

Clock type assignment
Identifies a time source for setting the logical partition's time-of-day (TOD) clock.

The logical partition's clock is synchronized with the central processor complex time-of-day clock (CPC TOD clock). Ordinarily, the logical partition's clock is set to the same time as the CPC's time source (either the CPC TOD clock or an external time reference, such as a Sysplex Timer or Server Time Protocol (STP). But you can use this group box to select another source for setting the logical partition's clock.

Standard time of day
Indicates the logical partition's clock is set to the same time the CPC's time source (either the CPC TOD clock or an external time reference, such as the Sysplex Timer or STP).

Logical partition time offset
Indicates the logical partition's clock is set using an offset from the External Time Source's time of day.

Processor

This window displays information that determines the allocation and management of processor resources assigned to the logical partition activated by the profile.

Displays the logical partition's logical processor assignment.

Note: The **Mode** list on the **General** image page lists the operating modes. The logical partition operates in the selected mode upon being activated with this profile. Depending on the selected mode and what processors are installed in your system will determine the allocation and management of the processor resources.

You can find more detailed help on the following elements of this window:

Group name

Displays the group profile name assigned to the logical partition, A logical partition can be assigned to only one group.

Note: If the group profile name is blank, then the logical partition is not assigned to a group.

Logical processor assignment (CPs - General and SSC modes)

The logical partition's logical processor assignment identifies the number of logical processors and type of physical processors assigned to it and, if the logical partition shares other processors.

Identifies the type of physical processors assigned to the logical partition and determines which of the remaining controls complete the logical processor assignment.

Dedicated central processors
Indicates a central processor is dedicated to each logical processor.

Not dedicated central processors
Indicates the logical processors share *not dedicated central processors* (central processors that are not already dedicated to other activated logical partitions when the logical partition is activated).

Logical processor assignment (CPs/zIIPs - General mode)

The logical partition's logical processor assignment identifies the number of logical processors and type of physical processors assigned and if the logical partition shares other processors.

Identifies the type of physical processors assigned to the logical partition and determines which of the remaining controls complete the logical processor assignment.

Dedicated central processors
Indicates a central processor is dedicated to each logical processor.

Dedicated z Integrated Information Processors (zIIPs)
Indicates the selected z Integrated Information Processors (zIIPs) are assigned to each logical processor.

Not dedicated central processors
Indicates the logical processors share *not dedicated central processors* (central processors that are not already dedicated to other activated logical partitions when the logical partition is activated).

Not dedicated z Integrated Information Processors (zIIPs)
Indicates the logical processors share not dedicated z Integrated Information Processors (zIIPs) (zIIPs that are not already dedicated to other activated logical partitions when this logical partition is activated).

Logical processor assignment (CPs/ICFs - Coupling facility mode)

The logical partition's logical processor assignment identifies the number of logical processors and type of physical processors assigned to it and, if the logical partition shares other processors.

Identifies the type of physical processors assigned to the logical partition and determines which of the remaining controls complete the logical processor assignment.

Dedicated central processors
Indicates that a central processor is dedicated to each logical processor.

Dedicated internal coupling facility processors
Indicates *Dedicated internal coupling facility processors* are dedicated to each logical processor.

Not dedicated central processors
Indicates the logical processors share *not dedicated central processors* (central processors that are not already dedicated to other activated logical partitions when this logical partition is activated).

Not dedicated internal coupling facility processors
Indicates the logical processors share *not dedicated internal coupling facility processors* (internal coupling facility processors that are not already dedicated to other activated logical partitions when this logical partition is activated).

Dedicated internal coupling facility processors and not dedicated central processors
Indicates the selected *Dedicated internal coupling facility processors* and *not dedicated central processors* are assigned to the logical partition.

Dedicated and not dedicated internal coupling facility processors
Indicates the selected *Dedicated and not dedicated internal coupling facility processors* and *not dedicated central processors* are assigned the logical partition

Logical processor assignment (CPs/IFLs - Linux only mode)

The logical partition's logical processor assignment identifies the number of logical processors and type of physical processors assigned to it and, if the logical partition shares other processors.

Identifies the type of physical processors assigned to the logical partition and determines which of the remaining controls complete the logical processor assignment.

Dedicated central processors
Indicates the selected central processor is dedicated to each logical processor.

Dedicated integrated facility for Linux
Indicates the selected *Dedicated integrated facility for Linux* processors are dedicated to each logical processor.

Not dedicated central processors
Indicates the selected logical processors share *not dedicated central processors* (central processors that are not already dedicated to other activated logical partitions when this logical partition is activated).

Not dedicated integrated facilities for Linux
Indicates the selected logical processors share *not dedicated integrated facilities for Linux* (Integrated Facilities for Linux (IFL) that are not already dedicated to other activated logical partitions when this logical partition is activated).

Logical processor assignment (CPs/zIIPs/ICFs/IFLs - z/VM mode)

The logical partition's logical processor assignment identifies the number of logical processors and type of physical processors assigned to it and, if the logical partition shares other processors.

Identifies the type of physical processors assigned to the logical partition and determines which of the remaining controls complete the logical processor assignment.

Dedicated central processors
Indicates the selected central processor is dedicated to each logical processor.

Dedicated z Integrated Information Processors (zIIPs)
Indicates the selected z Integrated Information Processors (zIIPs) are assigned to each logical processor.

Dedicated internal coupling facility processors
Indicates the selected *internal coupling facility processors* are assigned to each logical processor.

Dedicated integrated facilities for Linux
Indicates the selected *integrated facilities for Linux* are assigned to each logical processor.

Not dedicated central processors
Indicates the selected logical processors share *not dedicated central processor*s (central processors that are not already dedicated to other activated logical partitions when this logical partition is activated).

Not dedicated z Integrated Information Processors (zIIPs)
Indicates the selected logical processors share not dedicated z Integrated Information Processors (zIIPs) (zIIPs that are not already dedicated to other activated logical partitions when this logical partition is activated).

Not dedicated internal coupling facility processors
Indicates the selected logical processors share *not dedicated internal coupling facility processors* (internal coupling facility processors that are not already dedicated to other activated logical partitions when this logical partition is activated).

Not dedicated integrated facilities for Linux
Indicates the selected logical processors share *not dedicated integrated facilities for Linux* (integrated facilities for Linux that are not already dedicated to other activated logical partitions when this logical partition is activated).

Number of processors (General, Coupling facility, Linux only, and SSC modes)

Displays the number of processors that are used each time you activate a partition.

A *logical processor* is the processor resource defined to operate in a logical partition as a physical processor. A logical partition's control program uses its logical processors to perform jobs for the logical partition.

Initial
Indicates the number of logical processors to assign to the logical partition.

The number of processors can be from one to the maximum number of physical processors available to the logical partition. The maximum number of processors available is limited by:

- The number of physical processors configured an available.
- The number of processors supported by the operating mode selected on the **General** image page.
- The number of processors that are not already dedicated to another active logical partition at the time of the next activation.
- The number of processors supported by the control program at the time of the next activation.

Reserved
Indicates the number of reserved processors available that you want assigned to the logical partition.

Reserved processors can be configured online at a later time. Reserved processors can be defined at partition activation time, but are not used during partition activation. Instead, they are configured offline during activation automatically, and can be manually configured online. The reserved processor may or may not be available when the system is activated. If it is not available when the system is activated, it can become available during concurrent upgrade.

The ability to add and remove dedicated processors does not require deactivating/activating the partitions. This support is not restricted to concurrent upgrade purposes.

Note: This field is application only when the following selection is made:

- **Dedicated central processors**
- **Not dedicated central processors**
- **Dedicated internal coupling facility processors**
- **Not dedicated internal coupling facility processors**
- **Dedicated integrated facility for Linux**
- **Not dedicated integrated facility for Linux**

Processor type (General, z/VM, and Coupling facility modes)

Displays the number of processors that are used each time you activate a partition.

A *logical processor* is the processor resource defined to operate in a logical partition as a physical processor. A logical partition's control program uses its logical processors to perform jobs for the logical partition.

Initial
Displays the number of logical processors to assign to the logical partition.

The number of processors can be from one to the maximum number of physical processors available to the logical partition. The maximum number of processors available is limited by:

- The number of physical processors configured an available.
- The number of processors supported by the operating mode selected on the **General** image page.
- The number of processors that are not already dedicated to another active logical partition at the time of the next activation.
- The number of processors supported by the control program at the time of the next activation.

Reserved
Displays the number of reserved processors available that you want assigned to the logical partition.

Reserved processors can be configured online at a later time. Reserved processors can be defined at partition activation time, but are not used during partition activation. Instead, they are configured offline during activation automatically, and can be manually configured online. The reserved processor may or may not be available when the system is activated. If it is not available when the system is activated, it can become available during concurrent upgrade.

The ability to add and remove dedicated processors does not require deactivating/activating the partitions. This support is not restricted to concurrent upgrade purposes.

Note: This field is application only when the following selection is made:

- **Dedicated internal coupling facility processors and not dedicated central processors**
- **Dedicated and not dedicated internal coupling facility processors**

Not dedicated processor details (General, Coupling facility, Linux only, z/VM, and SSC modes)

Displays the initial processing weight, minimum and maximum processing weight, whether initial capping and workload manager are enabled, and absolute capping.

Initial processing weight

Displays the logical partition's processing weight for sharing the not dedicated processors.

The *not dedicated* processors are processors not already dedicated to other activated logical partitions when this logical partition is activated. This logical partition's *processing weight* is its share of the not dedicated processors. The processing weight can be from 1 to 999.

The exact percentage of the not dedicated processors allocated to the logical partition depends upon the processing weights of other logical partitions defined and activated on the same Central Processor Complex (CPC). That percentage is calculated by dividing the logical partition processing weight by the sum of the processing weights of all active logical partitions on the CPC.

A processing weight is a target, not a limit. It represents the share of the not dedicated processor resources guaranteed to a logical partition when all the resources are in use. When resources are available, this logical partition can borrow them if necessary. When this logical partition is not using its share of the resources, other logical partitions can use those resources.

Notes:

1. While excess resources are available, processing weights have no effect on how those resources are used. Weights take effect when the number of logical processors requiring a timeslice is greater than the number of not central processors.
2. This field is available only when either of the following selections are made:
   - **Not dedicated central processors**
   - **Not dedicated internal coupling facility processors**
   - **Dedicated internal coupling facility processors and not dedicated central processors**

     Note: This option is only available on the console for Version 2.10.2 and earlier.
   - **Not dedicated integrated facility for Linux**
   - **Not dedicated z Integrated Information Processors (zIIPs)**

   Otherwise, this field is unavailable.

Initial capping

Indicates the logical partition is prevented from using the not dedicated processors in excess of its processing weight.

Indicates logical partition *cannot* use the not dedicated processors in excess of its processing weight. That is, the processing weight is capped.

Otherwise, it indicates it can use the not dedicated processors in excess of its processing weight when the resources are not in use by another logical partition. That is, the processing weight is not capped.

The *Not dedicated processors* are processors not already dedicated to other activated logical partitions when this logical partition is activated. This logical partition's *processing weight* is its share of the not dedicated processors. Ordinarily, a processing weight is a target, not a limit. When the processing weight is *capped*, it is a limit.

Note: If this logical partition's share of the not dedicated processors is capped, it does not affect the shares set for other activated logical partitions.

This field is available only when either of the following selections are made:

- **Not dedicated central processors**
- **Not dedicated integrated coupling facility processors**
- **Dedicated integrated coupling facility processors and not dedicated central processors**

  Note: This option is only available on the console for Version 2.10.2 and earlier.
- **Dedicated and not dedicated internal coupling facility processors**

  Note: This option is only available on the console for Version 2.10.2 and earlier.

- **Not dedicated Integrated Facility for Linux**
- **Not dedicated z Integrated Information Processors (zIIPs)**. Otherwise, this field is unavailable.

Otherwise, this field is unavailable.

Enable workload manager

Indicates either **Enable workload manager** or **Initial capping** is enabled, but not both.

Displays the minimum and maximum processing weights.

This field is available only when either of the following selections are made:

- **Not dedicated integrated facility for Linux**
- **Not dedicated central processors**
- **zEnterprise Application Assist Processors (zAAPs)**

  Note: This option is available on the Hardware Management Console Version 2.12.1 and earlier.
- **Not dedicated z Integrated Information Processors (zIIPs)**

Otherwise, this field is unavailable.

Absolute Capping

Indicates the logical partition *can* use the not dedicated processors absolute capping number to limit the logical partition's activity. The absolute capping value is either None or a number of processors value from 0.01 to 255.0 specified.

Otherwise, it indicates the logical partition *cannot* use the not dedicated processors absolute capping when the resources are in use by another logical partition. That is, the processing absolute number is not capped.

The *Not dedicated processors* are processors not already dedicated to other activated logical partitions when this logical partition is activated. This logical partition's *absolute capping* is its share of the not dedicated processors. When the absolute processing value is *capped*, it is a limit.

Notes:

- If this logical partition's share of the not dedicated processors is capped, it does not affect the shares set for other activated logical partitions.
- This field is available only when either of the following selections are made:
  - **Not dedicated central processors**
  - **Not dedicated integrated coupling facility processors**
  - **Not dedicated integrated facility for Linux**
  - **Not dedicated z Integrated Information Processors (zIIPs)**

  Otherwise, this field is unavailable.

Security

Displays settings that determine the extent of interaction between the logical partition activated by the profile and other logical partitions activated on the same Central Processor Complex (CPC).

Partition security options

Displays the security options for the logical partitions activated by the profile.

Global performance data control
: Indicates whether the logical partition can be used to view the processing unit activity data for all other logical partitions activated on the same CPC.

Input/output (I/O) configuration control
Indicates whether the logical partition can be used to read and write any Input/Output Configuration Data Set (IOCDS) in the configuration.

This option indicates the logical partition can also be used to change the input/output (I/O) configuration dynamically and controls whether or not a logical partition can enter configuration mode.

Cross partition authority
Indicates whether the logical partition can be used to issue control program instructions that reset or deactivate other logical.

Logical partition isolation
Indicates whether reconfigurable channel paths assigned to the logical partition are reserved for its exclusive use.

When selected, channel paths are configured off; they will not become available to other logical partitions.

When not selected, reconfigurable channel paths assigned to this logical partition are not reserved for its exclusive use. Its channel paths can be configured off and reassigned to other logical partitions.

Counter facility security options

Displays the security options for the logical partitions activated by the profile.

Basic counter set authorization control
Indicates whether authorization is allowed to use the basic counter set. The set can be used in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is running.

Problem state counter set authorization control
Indicates whether authorization is allowed to use the problem-state counter set. The set can be used in analysis of cache performance, cycle counts, and instruction counts while the logical CPU is in problem state.

Crypto activity counter set authorization control
Indicates whether authorization is allowed to use the crypto-activity counter set. The set can be used to identify the crypto activities contributed by the logical CPU and the blocking effects on the logical CPU.

Extended counter set authorization control
Indicates whether authorization is allowed to use the extended counter set, The counters of this set are model dependent.

Sampling facility security options

Specifies the sampling facility security options for the logical partitions activated by the profile.

Basic sampling authorization control
Indicates whether authorization is allowed to use the basic-sampling function. The sample data includes an instruction address, the primary ASN, and some state information about the CPU. This allows tooling programs to map instruction addresses into modules or tasks, and facilitates determination of hot spots.

CP assist for cryptographic functions

Specifies the CP Assist Cryptographic Functions (CPACF) for the logical partitions activated by the profile.

Permit AES key import functions
Displays the current AES key import functions setting for CPACF when the logical partition is activated.

Permit DEA key import functions
Displays the current DEA key import functions setting for CPACF when the logical partition is activated.

Permit ECC key import functions
Displays the current Elliptical Curve Cryptography (ECC) key import functions setting for CPACF when the logical partition is activated.

Storage

Displays the amount of storage assigned to the logical partition activated by the profile. Logical partition storage allocation is composed of central storage assignments and expanded storage assignments.

Central storage

Central storage is the amount of storage that is available to allocate for main storage.

Amount in
Displays the amount of storage that is installed in the selected partition.

Initial
Displays the amount of central storage to allocate to the logical partition upon activation.

Initial storage is allocated to a logical partition in a contiguous block of one Gigabyte (GB) units. The logical partition has exclusive use of its initial storage. That is, it is not shared with other active logical partitions.

You must allocate at least 64MB of initial storage when the logical partition will operate in coupling facility mode. Otherwise, for any other operating mode, you must allocate at least 1 MB of initial storage.

Reserved
Displays the amount of central storage that can be reconfigured dynamically to the logical partition after activation. This field is only active if the operating mode selected on the **General** image page is **General**, **LINUX only**, or **z/VM** mode. It is not available in coupling facility mode.

Reserved storage is allocated to a logical partition in a contiguous block of one Gigabyte (GB) units, and is contiguous to an located above its initial storage. But, unlike its initial storage, the logical partition does not have exclusive use of its reserved storage. The reserved storage provides the logical partition wit an additional amount of storage to use only if it is not already being used by another active logical partition.

The is no minimum for reserved storage. Zero gigabytes (0 GB) is a valid amount of reserved storage.

Storage origin
Displays how the central storage origin is determined.

Determined by the system
Displays the Central Processor Complex (CPC) determine the central storage origin.

The CPC allocates central storage, wherever sufficient, contiguous space is available.

Determined by the user
Indicates the selected central storage origin is established in this profile.

Origin
Displays the megabyte where storage allocation begins when the central storage origin is determined by the user through this profile.

When this profile is used to activate a logical partition, sufficient and contiguous space must be available from the origin for the amount of central storage specified. Logical partition activation fails if sufficient storage is not available from the origin, regardless of whether the origin is determined by the system or by the user through this profile.

Virtual Flash Memory

Displays the amount and Virtual Flash Memory storage allocated to the logical partition. The virtual memory increments in 16 GB amounts with a maximum of 6144 GB.

Initial
Displays the initial amount of virtual flash memory for the selected partition in 16 GB increments.

Maximum
Displays the maximum amount of virtual flash memory to a allow for the selected partition.

Options

Displays the image options for the processor values on this window:

Minimum and Maximum I/O priority values can be specified at a partition level. These minimum and maximum I/O priority values can both be set at partition activation time or dynamically (post partition activation).

Minimum I/O priority
The minimum value must be less than or equal to the maximum value entered. This value can range from 0 to the maximum I/O priority allowed for that processor.

The minimum default is a priority value of 0.

Maximum I/O priority
This maximum processor I/O priority is obtained from new System Information support.

The maximum default is a priority value of 0.

Defined capacity
The measure of processor resource consumption for a logical partition, expressed in millions of service units (MSU) per hour.

CP management cluster name
The name specified for the CP management cluster.

SSC

This window displays the configuration settings for the selected logical partition in IBM Secure Service Container (Secure Service Container) mode.

Note: Cryptographic (CRYPTO) options can be selected for the Secure Service Container partition.

The Secure Service Container configuration settings include the following:

Boot selection
Displays the Boot selection for the selected Secure Service Container partition.

Secure Service Container installer
Displays until the Secure Service Container partition is restarted and the input fields contain information that was previously defined.

Secure Service Container
Displays after the Secure Service Container partition is restarted. The **Reset Logon Settings** and **Reset Network Settings** can be updated after the restart.

Master user ID
Displays the master user ID for the selected Secure Service Container logical partition.

A master user ID can be from one to 32 characters long. It cannot have special characters or embedded blanks. Valid characters for a master user ID name are numbers **0** through **9**, alphabetic, period, underscores, and minus symbol.

Master password
Displays the master password for the master user ID you specified.

A master password can have a minimum of 8 characters and a maximum of 256 characters.

Confirm master password
Displays again the same master password you specified in the **Master password** field.

Host name
Displays the host name for the selected Secure Service Container logical partition.

A host name can be from one to 32 characters long. It cannot have special characters or embedded blanks. Valid characters for a host name are alphanumeric characters, periods (.), colons (:), and hyphens (-).

IPv4 gateway
Displays the default gateway IPv4 address for the selected Secure Service Container logical partition.

IPv6 gateway
Displays the default gateway IPv6 address for the selected Secure Service Container logical partition.

Network Adapters

The Network Adapters table displays the IP address and details settings for the Secure Service Container logical partition.

CHPID
Displays the CHPID for the selected Secure Service Container logical partition.

VLAN
Displays the VLAN for the selected Secure Service Container logical partition.

Port
Displays the Port 0/1 parameter for the selected Secure Service Container logical partition.

IP address
Displays the IPv4 or IPv6 address for the selected Secure Service Container logical partition. Also, indicates DHCP or Link Local if that is the specific IP address type.

Mask/Prefix
Displays the Mask/Prefix for the IPv4 or IPv6 address specified.

DNS Servers

The DNS Servers table displays the IPv4 or IPv6 address for the selected Secure Service Container logical partition.

DNS is a distributed database system for managing host names and their associated Internet Protocol (IP) addresses. Using DNS means that people can use names, such as "www.jkltoys.com" to locate a host, rather than using the IP address (xxx.xxx.xxx.xxx). A single server may only be responsible for knowing the host names and IP addresses for a small subset of a zone, but DNS servers can work together to map all host names to their IP addresses. DNS servers working together allow computers to communicate across the Internet.

IP address
Displays the current IPv4 or IPv6 address for the selected Secure Service Container logical partition.

Load

Displays information that controls loading a control program for the logical partition activated by the profile.

Note: The image pages do not include this additional page if the operating mode selected on the **General** image page is Coupling facility or SSC mode.

Load during activation
Indicates whether the load is performed during activation.

If it has been selected it indicates a load is performed. The other information on the window is used to perform the load. Otherwise, a load is not performed.

Device type
Indicates the type of device to perform a load for the logical partition. You would use the SCSI or NVMe option to do a standalone dump to a SCSI device or NVMe adapter.

ECKD
Indicates to perform an IPL on the logical partition from ECKD DASD device type.

SCSI
Indicates to perform an IPL on the logical partition from SCSI device type.

NVMe
Indicates to perform an IPL on the logical partition from NVMe device type.

Tape
Indicates to perform an IPL on the logical partition from Tape device type.

IPL type:
Indicates the type of IPL for the selected ECKD device type to perform for the logical partition.

Channel Command Word (CCW)
Indicates to perform the load on Channel Command Word (CCW).

List-directed
Indicates to perform the load on a list-directed IPL.

If the selected load type is **SCSI**, **NVMe**, or **Tape** this field is unavailable.

Load type:
Indicates the type of load to perform for the logical partition. You would use the **ECKD** or **Tape** option to do a standalone dump and select the **Load a dump program** option.

Load an OS
Indicates to perform an operating system load type on the logical partition.

Load a dump program
Indicates to perform a dump program load type on the logical partition.

Validation:

Enable Secure Boot
Indicates to verify the signature of the load program and distributor's signature match.

Certificates
Indicates the assigned certificates keys to enable a secure boot for the selected logical partition.

If the selected load type is **Tape** or **ECKD** and IPL type **CCW** is selected this field is unavailable.

Options:
Indicates whether the store status function stores the current values of the processing unit timer, the clock comparator, the program status word, and the contents of the processor registers in their assigned absolute storage locations.

- A check mark indicates performing the store status function before the load.
- An empty check box indicates not performing the store status function before the load.

If the selected load type is **SCSI** or **NVMe** this field is unavailable.

Load address:

Displays the address of the input/output (I/O) device that provides access to the control program to load. For a SCSI load or NVMe load, this field has the device number of the device (for example, fibre channel adapter) that is used to perform the SCSI or NVMe load. This should contain four hexadecimal digits for NVMe load or five hexadecimal digits for SCSI load.

A load address is required.

The source of the control program must be an I/O device in the I/O configuration that is active when this profile is activated. The I/O device can store the control program or can be used to read the control program from a data storage medium.

Note: This field is applicable only when **Use dynamically changed address** check box is empty. Otherwise, if the check box displays a check mark, this field is unavailable.

Use dynamically changed address

Indicates whether the load address is dynamically determined by changes to the channel subsystem Input/Output definition (I/O).

If this is selected, the load address is dynamically determined. Otherwise, this profile sets the load address. See the **Load address** field for the address set by this profile.

Load parameter:

Indicates the optional information, if any, to use to further control how the control program is loaded during activation.

Some control programs support the use of a load parameter to provide additional control over the performance or outcome of a load. Check the configuration programming and reference documentation for the control program to determine the load parameters that are available and their effects on a load.

Note: This field is applicable only when **Use dynamically changed parameter** is **not** selected. Otherwise, this field is unavailable.

Use dynamically changed parameter

Indicates whether the load parameter is dynamically determined by changes to the channel subsystem Input/Output (I/O) definition.

If this is selected, the load parameter is dynamically determined. Otherwise, this profile sets the load parameter. Enter the parameter for this profile in the **Load parameter** field.

Time-out value:

Indicates the amount of time to allow for the completion of the load.

If the load operation cannot be completed within the specified time, the operation is canceled.

If the selected load type is **SCSI**, **NVMe**, or **ECKD** and IPL type **List-directed** is selected, this field is unavailable.

Boot record location:

Indicates the boot record location for an ECKD DASD.

The boot record location (C,H,R format) parameters is specified from the volume label or be specified.

- The **use volume label**specifies the boot record label from the volume label
- Specified the C,H,R format. The Cylinder number is a 4-byte value ranging from '0x00000000' to '0x0FFFFFFF'. The Head number is a 1-byte value ranging from '0x00' to '0x0F'. The Record number is a 1-byte value ranging from '0x01' to '0xFF'.

If the selected load type is **SCSI**, **NVMe**, **Tape**, or **ECKD** and IPL type **CCW** is selected, this field is unavailable.

Worldwide port name:

Displays the Worldwide Port Number identifying the Fibre Channel port of the SCSI target device (according to the FCP/SCSI-3 specifications). This is a 64-bit binary number designating the port name, represented by 16 hexadecimal digits. This is required for SCSI load or SCSI dump.

If the selected load type is **ECKD**, **NVMe** or **Tape**, this field is unavailable.

Logical unit number:

Displays the number of the logical unit as defined by FCP (according to the FCP/SCSI-3 specifications). This is the 64-bit binary number designating the unit number of the FCP I/O device, represented by 16 hexadecimal digits. This field is required for SCSI load or SCSI dump.

If the selected load type is **ECKD**, **NVMe**, or **Tape**, this field is unavailable.

Boot program selector:

Displays the program to load from the FCP-load device and contains a decimal value in the range from 0 to 30.

If the selected load type is **Tape** or **ECKD** and IPL type **CCW** is selected, this field is unavailable.

Boot record logical block address:

Displays the load block address if your file system supports dual-boot or booting from one of the multiple partitions. If no block address is specified, the logical-block address of the boot record is assumed to be zero. This feature could be used to IPL using a second or backup boot record, in case the original one is corrupted or overwritten by accident.

This field is unavailable if a load type of **ECKD** or **Tape** are selected.

Operating system load parameters:

Displays a variable number of characters to be used by the program that is loaded. This information will be given to the IPLed operating system and will be ignored by the machine loader. The IPLed operating system (or standalone dump program) has to support this feature. Any line breaks you enter are transformed into spaces before being saved.

If the selected load type is **Tape** or **ECKD** and IPL type **CCW** is selected, this field is unavailable.

Crypto

This window displays information that controls how the logical partition activated by the profile uses the coprocessors and accelerators assigned to it. The settings are referred to here as *cryptographic controls*, and apply to the logical partition only if it is customized for using coprocessors and accelerators.

Control domain index

Displays the cryptographic domain index (CDX) numbers of one or more control domains for the logical partition.

A logical partition's *control domains* are those cryptographic domains for which remote secure administration functions can be established and administered from this logical partition.

But a logical partition's control domains can also include the usage domains of other logical partitions. Assigning multiple logical partitions' usage domains as control domains of a single logical partition allows using it to control their software setup.

If you are using the Integrated Cryptographic Service Facility (ICSF), select at least one control domain and matching usage domain. Refer to ICSF documentation for information about ICSF basic operations.

If you are using a Trusted Key Entry (TKE) workstation to manage cryptographic keys, the TKE documentation provides information about selecting control domains and usage domains for a logical partition that is a TKE host or a TKE target.

Control and Usage domain index

Displays the cryptographic domain index (CDX) numbers of one or more usage domains for the logical partition.

A logical partition's *control and usage domains* are domains in the cryptos that can be used for cryptographic functions. The usage domains cannot be removed if they are online.

A logical partition's control domains can also include the usage domains of other logical partitions. Assigning multiple logical partitions' usage domains as control domains of a single logical partition allows using it to control their software setup.

If you are using the Integrated Cryptographic Service Facility (ICSF), refer to ICSF documentation for information about ICSF basic operations.

If you are using a Trusted Key Entry (TKE) workstation to manage cryptographic keys, the TKE documentation provides information about selecting control domains and usage domains for a logical partition that is a TKE host or a TKE target.

Cryptographic candidate list

Identifies which coprocessors from the candidate and online list will be assigned to the logical partition at the next activation.

Cryptographic online list
Identifies which coprocessors from the candidate and online list will be brought online at the next activation.

The logical partition must be activated to bring the coprocessors or accelerators online.

Time Offset

This window displays the Central Processor (CPC) External Time Source settings and how it is applied when the logical partition's clock is set.

Note: The image profile includes this window only if the clock type selected on the **General** page of the logical partition's image profile is **Logical partition time offset**.

Offset
Indicates the number of days, hours, and minutes you want to set for the offset from the External Time Source's time of day. You can set an offset within the following range:

- 0 to 999 days
- 0 to 23 hours
- 0, 15, 30, or 45 minutes

days
Indicates the number of days, from 0 to 999, that you want to set for the offset from the External Time Source's time of day.

hours
Indicates the number of hours, from 0 to 23, that you want to set for the offset from the External Time Source's time of day.

minutes
Indicates the number of minutes, 0, 15, 30, or 45, that you want to set for the offset from the External Time Source's time of day.

Decrease system time value by the amount shown
Displays the logical partition's clock *back* setting from the External Time Source's time of day by the number of days, hours, and minutes in the offset.

Increase system time value by the amount shown
Displays the logical partition's clock *ahead* setting of the External Time Source's time of day by the number of days, hours, and minutes in the offset.

Help
To display help for the current window, click **Help**.

Group page

This window displays a group profile name, group description, and group capacity value used in determining the allocation and management of processor resources assigned to the logical partition in the group.

Make a selection from the Profile tree to view the group pages in the profile.

Group name
Displays a group name for logical partition(s) in the group.

Group description
Indicates information that describes the contents or purpose of the profile.

View Console Events

Accessing the View Console Events task

The Support Element console automatically keeps records of significant operations and activities, referred to as *console events*, performed either:

- Manually by a console operator.
- Through management-type Application Programming Interfaces (APIs) to the Support Element Console Application.
- Automatically by the Support Element Console Application.

Some console events simply indicate an operation or activity occurred. For example, a console event is logged when a console operator logs on the console.

Other console events are logged in pairs, to indicate when an operation or activity began and when it ended. For example, a console event is logged when a power-on reset is started, and another console event is logged when the power-on reset ends. Console events logged when an operation or activity ends typically also indicate whether the operation or activity succeeded or failed.

This task enables you to view a record of system events occurring on the Support Element console. System events are individual activities that indicate when processes occur, begin and end, succeed or fail.

When an event occurs, the date and time it occurs and a brief description of the event are recorded in the **Console Event Log**.

To view the console events:

1. Open the **View Console Events** task. The View Console Events window is displayed.

   Initially, all events in the table are displayed in descending order, from the most recent event to the oldest event. You can work with the table by using the table icons from the table toolbar. If you place your cursor over an icon a description of the icon is displayed. The icons perform the following functions:

   Show Filter Row
   Displays a row under the title row of the table. Select **Filter** found under a column title to define a filter for that column. This limits the entries in the table. Tables can be filtered to show only those entries most important to you. If you no longer want the **Filter** row to appear, click **Hide Filter Row**.

   Clear All Filters
   Returns the table back to the complete listing.

   Edit Sort
   Performs multi-column sorts of objects in the table in ascending or descending order. Click **OK** when you have defined your preferred order.

   Clear All Sorts
   Returns the table back to the default order.

   Quick Filter
   Allows you to select a filter category to apply to the filter. By default, all columns are filtered, showing only rows containing a cell whose value includes the filter text. When you click the drop-down arrow, a menu is displayed that allows you to restrict the columns to which the filter is applied.
2. When you have finished reviewing the console events, click **Cancel**.

View Console Events

This task displays console events logged by the console.

The console automatically keeps a log of significant operations and activities, referred to as *console events*, that occur while the application is running.

This window initially displays all console events currently logged and lists them in reverse order of occurrence (from the most recent event to the oldest event).

A filter task bar appears above the table that allows you to change the information that you want displayed, such as, changing the number of events listed or the order of the events.

Events table

This table initially displays the console events in descending order with the following information:

Date
Displays the date and time when the console event occurred. Use the up or down arrow to display the table in ascending or descending order by the date.

Events
Describes the console event logged by the console. Use the up or down arrow to display the table in alphabetical order or reverse alphabetical order by the console event.

You can work with the table by using the filter icons on the task bar above the table. If you place your cursor over an icon the icon description appears.

Filter task bar

The filter task bar includes table filter icons that perform the following functions:

Show Filter Row
Displays a row under the title row of the table. Select **Filter** found under a column title to define a filter for that column. This limits the entries in the table. Tables can be filtered to show only those entries most important to you.

Note: As you are filtering, the information on the bottom of the table indicates the total number of items you are working with and the number of items filtered and displayed.

The filter conditions on **Date** include the following:

All Dates
Displays all events for all dates.

Dates until
Displays only those events up to the date and time you selected.

Dates from
Displays only those events from the current date to the date and time you selected.

Dates between
Displays only those events within the beginning and ending dates and times you selected.

The filter conditions on **Events** include the following (each condition allows you to specify text that should be sorted on and whether or not to match the case of the text being sorted on):

Contains
Displays only those events that includes the **Text** that you specified.

Does not contain
Displays only those events that does not include the **Text** that you specified.

Starts with
Displays only those events that have an event name that begins with the **Text** that you specified.

Ends with
Displays only those events that have an event name that ends with the **Text** that you specified.

Matches
Displays only those events that exactly matches the complete event name that you specified.

Is empty
No events are displayed in the table.

Is not empty
All events are displayed in the table.

Click **OK** when you have defined your filter. The filtered view can be toggled on and off by selecting the check box next to the desired filter in the filter row. If you no longer want the **Filter** row to appear, click **Hide Filter Row**.

Clear All Filters
Returns the table back to the complete listing.

Edit Sort
Performs multi-column sorts of objects in the table in ascending or descending order. Click **OK** when you have defined your preferred order.

Clear All Sorts
Returns the table back to the default order.

Quick Filter
Allows you to select a filter category to apply to the filter. By default, all the columns are filtered, showing only rows containing a cell whose value includes the filter text. When you click the drop-down arrow, a menu is displayed that allows you to restrict the columns to which the filter is applied.

Max page size

Specify the number of entries in the input field that you want displayed at one time in the table, then press Enter. If the total number of events exceed the number that appear in the table you can specify a page number in the entry field to see more entries or click the forward or backward arrows to page through the additional entries. The amount of entries that are displayed is the number you specified in the **Max Page Size** input field.

Note: The maximum page size allowed is 999.

Additional functions from this window include:

Cancel
To close this window when you are done viewing this information, click **Cancel**.

Refresh
To update the table with the most recent events and restore the table defaults, click **Refresh**.

Help
To display help for the current window, click **Help**.

View Console Tasks Performed

Accessing the View Console Tasks Performed task

This task allows the support system to review the tasks that have been performed on a Hardware Management Console. This can be very helpful when working with an operator to determine what happened if a problem occurs.

To view the console tasks performed:

1. Open the **View Console Tasks Performed** task. The View Console Tasks Performed window is displayed.
2. A table of information that includes the last 2000 tasks performed on the Hardware Management Console is displayed. The table includes the task name, user ID that accessed the task, and the user interface style that was used.
3. Click **OK** when you are done viewing the information.

View Frame Layout

Accessing the View Frame Layout task

This task provides a graphic view of the physical location of the hardware objects that are defined to this Hardware Management Console. Each object is shown with its frame designation and position within the frame. By opening (double-clicking on) the object, additional information is provided:

- Machine type
- Model

- Serial number
- Device location

Objects can be added, removed, or moved by a user with service representative roles using the **Edit Frame Layout** task.

To view the physical location of hardware objects that are defined to the Hardware Management Console:

1. Open the **View Frame Layout** task. The View Frame Layout window is displayed.

   Note: If you select more than one object, the Object Selection window is displayed prompting you to select a single CPC on which to perform the task.
2. Click **OK** when you are done viewing the frame layout.

View Frame Layout

This window graphically displays the physical location of the hardware objects that are defined to this Hardware Management Console. Each object is shown with its frame designation and position within the frame.

Additional information includes:

- Machine type
- Model
- Serial number
- Device location

Use the mouse to select graphics and to display pop-up menus of views you can use on the selected graphic. The possible menu choices available for viewing include:

- Device details
- Support element details

If you are assigned a user ID with service representative task roles, you can add, remove, or move objects by using the **Edit Frame Layout** task.

Additional functions are available from this window:

OK
To close the window, click **Cancel**.

Cancel
To close the window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Device/CPC Details

Use this window to view device/CPC details. Detailed hardware configuration information for a selected device is displayed.

To change the device details, specify the device serial number and select the associated CPC, then click **Change Device Details**.

Device
Displays the name or type of the device.

Description
Displays a brief description of the device.

Location
Identifies the location of the device.

Serial number
Displays the serial number of the device.

Associated CPC
Displays the name and location of the Central Processor Complex (CPC) that the device is physically connected to.

The CPC you select becomes associated with the device. The hardware configuration information for a machine is stored on the support elements of its CPCs. A Support Element stores information only for its CPC and the devices associated with the CPC.

Associating a device with a CPC is necessary to identify the Support Element used for storing the device information, and to indicate the device is physically connected to the CPC. But associating a device with a CPC does not affect which CPCs can be configured to use the device.

OK

When you are done reviewing the information in this window, click **OK**.

Help
To display help for the current window, click **Help**.

Support Element Details

Use this window to confirm the Support Elements listed by description, serial number, and location and associated with a specific CPC.

This is the Central Processor Complex (CPC) that the device is physically connected to.

The CPC you select becomes associated with the device. The hardware configuration information for a machine is stored on the Support Elements of its CPCs. A support element stores information only for its CPC and the devices associated with the CPC.

Associating a device with a CPC is necessary to identify the Support Element used for storing the device information, and to indicate the device is physically connected to the CPC. But associating a device with a CPC does not affect which CPCs can be configured to use the device.

To confirm the Support Elements, click **OK**.

OK
When you are done reviewing the information in this window, click **OK**.

Help
To display help for the current window, click **Help**.

View Hardware Configuration

Accessing the View Hardware Configuration task

Hardware configuration information stored on the Support Element of the system is information about the system's frame and parts in the frame. Information about the frame includes the machine type, model number, and serial number of the frame's machine, and the system's location in the frame. The information for each part in the frame includes its:

- Location
- Custom card identifier (CCIN)
- Description
- Part number
- Serial number
- Engineering change (EC) number

You can use the Support Element workplace to display the hardware configuration information.

To view the hardware configuration:

1. Open the **View Hardware Configuration** task.

Information is displayed about the system's frame and lists the location, CCIN, and a description of each part in the frame.

Use the online Help for more information about the display fields and list.

2. To display the part number, serial number, and EC number for a specific part, select the part from the list, then click **Details**.

   This displays the selected part's detailed information on the Part Details window.

View Hardware Configuration

This window displays information that describes a frame and the parts in the configuration of a system, and optional expansion drawer(s), if installed. Parts may be cards or features.

Use the window to view additional part details by clicking a part from the list.

Machine Type - Model
Displays the machine type and model number of the machine (system location) the frame is in.

Machine serial number
Displays the serial number of the machine the frame is in.

Processor location
There is no single system processor location or FRU, so this field simply displays the generic location of ASYS.

Location
Displays the physical **part location** in the system processor.

The **part location** identifies the location of a part in a frame.

Parts can be located in the power module section or card section within a system or in optional expansion drawers.

Part locations are identified by up to twelve characters. Some parts, like cables, are identified by up to twelve characters for the location of each end, with the two locations separated by a dash.

The first character of a twelve character location identifies the frame location.

A
Identifies the rightmost frame in the machine

Z, Y, X, W, or V
Identify frames attached to the left of frame A.

Note: The identifiers used for additional frames are determined by the machine model.

The next three characters identify the location of the system or expansion drawer within the frame.

01A
Indicates the location is the bottom of the frame.

42A
Indicates the location is the top of the frame.

The remaining four to eight characters identify the type of part, and indicate where the part is located within the system or expansion drawer.

- For the following parts in the card section, 'nn' identifies the card socket where the part is located:

  LGnn
  FICON channel card

  LGnn
  Logic card

Example A logic card in card socket 26 of the system or expansion drawer at the bottom of frame Z is identified by part location:

- Z01ALG26

- For the following parts in the power module section, 'nn' is a number that distinguishes a module from other modules of the same type:

  PSnn
  Bulk power controller

  PSnn
  Bulk power regulator

- **Example** The two bulk power controllers are idendified by part locations:
  - Z29BPS03 - side A Z29BPS13 - side B

Details...
To display additional information on a specific part, click **Details**.

Cancel
To close this window, click **Cancel**.

Help
To display help for the current window, click **Help**.

Part Details

This window displays information that describes and identifies a part. Parts may be cards or features.

Part ID
Displays the custom card identification number (CCIN).

Part description
Displays a description of the part.

Part type
Displays the part type.

Location
Displays the physical part location.

Part number
Displays the part number.

Serial number
Displays the serial number.

Engineering change number
Displays the engineering change (EC) number.

OK
To close this window and return to the previous window, click **OK**.

Help
To display help for the current window, click **Help**.

View Internal Code Changes Summary

Accessing View Internal Code Changes Summary task

To view a summary of internal code changes, open the **View Internal Code Changes Summary** task. The View Internal Code Change Summary window is displayed.

View Internal Code Changes Summary

You can use this task to view a summary of internal code changes pending conditions that would otherwise require running the separate tasks to obtain the information. The following areas indicate whether a pending condition displays and a link to the specific task:

- Manage Adapter Firmware
- Query Coupling Facility Reactivations
- Query Internal Code Changes Pending Power on Reset

- Manage PCI System Services
- Update PCI Adapter Internal Code

Close
To close this window and exit this task, click **Close**.

Refresh
To update the displayed internal code change summary information with the information, click **Refresh**.

Help
To display help for the current window, click **Help**.

View Licenses

Accessing the View Licenses task

This task allows you to view the Licensed Internal Code (LIC) that you have agreed to for this Support Element console. This list does not include program and code provided under separate license agreements. This task window appears after the initialization window or to view the license.

To view the licenses:

1. A list of the licenses is displayed, click on any of the license links for more information.

   Note: This list does not include programs and code provided under separate license agreements.
2. Click **OK** when you are done viewing this information.

View LPAR Cryptographic Controls

Accessing the View LPAR Cryptographic Controls task

You can use this task to review information about the active logical partitions that use the Crypto Express features assigned to them. You can review:

- A summary tab page of information on all active logical partitions.
- Individual tab pages for each logical partition's cryptographic controls.

To review the logical partition's cryptographic controls:

1. Open the **View LPAR Cryptographic Controls** task.

   The View LPAR Cryptographic Controls window displays. The window includes a summarized view tab for cryptos on all partitions and individual tabs for each logical partition's cryptographic controls.
2. Click **OK** when you have finished.

View LPAR Cryptographic Controls

Use the **View LPAR Cryptographic Controls** task to review the cryptographic candidate list and usage domain index assignments for the logical partitions that use the Crypto Express feature.

Click the tab along the right hand side of the window to display:

- A summary page of cryptographic candidate list and usage domain index assignments for all logical partitions.
- An individual page for each active logical partition that describes the assignment of the control domain index, the usage domain index, the cryptographic candidate list, and the cryptographic online list from the activation profile.

Additional functions on this window include:

Close
To close the window, and return to the window from which you selected the task, click **Close**.

Refresh
To update the current window with the new changes, click **Refresh**.

Help
To display help for the current window, click **Help**.

Conflicts

This window displays a list of the inactive partitions that will create conflicts with activated partitions if they become activated. The inactive partitions listed could be in conflict with other inactive partitions in the list if they become activated.

Crypto numbers in conflict
Displays the inactive crypto numbers that will create conflicts with the activated partitions.

Usage domains in conflict
Displays the inactive usage domain numbers that will create conflicts with the activated partitions.

Close
To exit the current window, click **Close**

Help
To display help for the current window, click **Help**.

Summary page

The summary page displays the installed cryptos and cryptographic settings for all logical partitions. The cryptographic settings on the summary page include the cryptographic candidate list and usage domain index assignments. For active partitions, the cryptographic settings currently in effect are displayed. For inactive partitions, the cryptographic settings in the activation profile are displayed. Select the “Conflicts” on page 968 link to display the inactive partitions that will be in conflict when activated with existing activated partitions.

You can work with the table by using the table icon or **Select Action** list from the table tool bar. If you place your cursor over an icon, the icon description appears.

Configure Columns
Allows you to select which columns you want displayed. Arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the **Columns** list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the list box and using the arrow buttons to the right of the list to change the order of the selected column.

Individual pages

Each page of the View LPAR Cryptographic Controls displays the cryptographic settings for an active logical partition. The page tab displays the active logical partition's name.

The cryptographic controls on each page indicate the current settings of each active logical partition's cryptographic controls. You can find more detailed help on the following elements of this window:

Control domain index

Displays the cryptographic domain number the active logical partition uses for remote secure administration functions.

A logical partition's control domains can also include the usage domains of other logical partitions. Assigning multiple logical partitions' usage domains as control domains of a single logical partition allows using it to control their software setup.

If you are using the Integrated Cryptographic Service Facility (ICSF), there is at least one control domain and matching usage domain. Refer to ICSF documentation for information about ICSF basic operations.

If you are using a Trusted Key Entry (TKE) workstation to manage cryptographic keys, the TKE documentation provides information about control domains and usage domains for a logical partition that is a TKE host or a TKE target.

Usage domain index

Displays the usage domain number the active logical partition uses for Public Key Algorithm (PKA) and cryptographic functions.

If you are using the Integrated Cryptographic Service Facility (ICSF), there is at least one control domain and matching usage domain. Refer to ICSF documentation for information about ICSF basic operations.

If you are using a Trusted Key Entry (TKE) workstation to manage cryptographic keys, the TKE documentation provides information about control domains and usage domains for a logical partition that is a TKE host or a TKE target.

Cryptographic candidate list

The candidate list identifies which coprocessors will be assigned to the partition at the next activation. For each selected coprocessor in the candidate list, there is a corresponding coprocessor selected in the online list.

Cryptographic online list

The online list identifies which coprocessors will be configured online at the next activation of the logical partition, as specified in the activation profile. For each selected coprocessor in the online list, there is a corresponding coprocessor selected in the candidate list.

You must activate the partition to bring the coprocessors or accelerators online.

View Partition Resource Assignments

Accessing the View Partition Resource Assignments task

You can use the console to view the mapping of active logical partitions and associated processor information.

Note: Use this task under the direction of product support.

To view the resource assignments for partitions:

1. Open the **View Partition Resource Assignments** task. The View Partition Resource Assignments window displays.
2. The window displays the active logical partitions and physical processors associated with each active logical partition.

View Partition Resource Assignments

Use this task, under the direction of product support, to view the mapping of active logical partitions and associated processor information.

You can work with the table by using the table icons or **Actions** list from the table toolbar. If you place your cursor over an icon, the icon description is displayed. The following functions are available from the table toolbar:

Spare 

Select this icon toggle to display or hide shared, unassigned, and spare physical processor assignments.

Pause/Resume  **/**
image icon of pause and resume button
Select these icons to dynamically pause or resume the current view of the logical partition resource assignments.

Export 
Select this option from the **Actions** list or click **Export** icon.

Export as HTML
Downloads table data into a Hypertext Markup Language (HTML) file. This action is only available when you are using a remote browser.

Export All to CSV
Downloads table data into a Coma Separated Values (CSV) file. You can then import the downloaded CSV file into most spreadsheet applications. This action is only available when you are using a remote browser.

Print 
Select this option from the **Actions** list or click **Print** icon.

Print All
Prints all rows in the table. This action is only available when you are using a remote browser.

Print Selected
Prints selected rows in the table. This action is only available when you are using a remote browser.

Print Preview
Displays a printable version of all rows in the table. This action is only available when you are using a remote browser.

Expand All
Expands the Node and Chip view and displays physical processor type details for each Chip assigned to the active logical partitions. The core ID is identified with each Chip.

Collapse All
Collapses the Node and Chip details view for the active logical partitions. Displays the Chip summary view of processor types assigned to the active logical partitions. This is the default.

Partition Resource Assignment table

Use the Partition Resource Assignment table, under the direction of product support, to view processor allocations to partitions in your system. The active logical partitions are identified at the top of the table. The Node and Chip numbers associated with each active logical partition are identified on the left. You can view the Node and Chips assignments using the **Expand All** and **Collapse All** icons to view or hide sections.

To view the resource assignments for partitions:

Logical partition name
Displays the active logical partition and if Hyperdispatch (HD) is enabled.

Node
Displays the processor Node number in your system.

Chip
Displays the processor Chip number associated with the Node and lists the processor types associated with each active logical partitions. The Chip **Collapse All** icon displays a summary view. The following physical processor types are:

- General processors (G)

- Coupling facility processors (C)
- Integrated Facilities for Linux (IFLs) (I).
- z Integrated Information Processors (zIIPs) (Z).
- Integrated Firmware Processor (IFPs) (F)

The physical processor types may have some of the following conditions:

- Indicates the physical processor types are shared (SH).
- Indicates the physical processor is dedicated (D).
- Indicates the vertical polarity for the physical processor types (H/M/L).

Additional functions on this window include:

Close
To exit the current window, click **Close**.

Help
To display help for the current window, click **Help**.

View Security Logs

Accessing the View Security Logs task

This task allows you to view the security events logged for the Support Element console. A security event occurs when an object's operational state, status, or settings change or involves user access to tasks, actions, and objects.

To view a security log:

1. Open the **View Security Logs** task. The View Security Logs window is displayed.
2. When you are done viewing the security log and ready to exit the task, click **File**, **Exit**.

View Security Logs

Use this task to view the console's default security log.

The console automatically keeps a *default security log* of security events that occur while the console application is running. A *security event* occurs when a task is performed that either:

- Changes an object's operational state, status, or settings. For example, activating a CPC, customizing an activation profile, and loading a CPC image.
- Or involves user access to console tasks, actions, and objects. For example, logging on and off are security events.

On the menu bar:

- Click **Search By** to search the security log that is currently open, then select the following:
  - Date to search for events by the time and date they occurred.
  - Event to search for an event by its description.
  - Category to search for events by a certain category.
  - User to search for events by a user ID.
- Click **Options** to view or alter the security log options, then select the following:
  - **Create hardware message when approaching maximum size, On** to enable the creation of a hardware message when the security log is approaching the maximum size.
  - **Create hardware message when approaching maximum size, Off** to disable the creation of a hardware message when the security log is approaching the maximum size.

- **Log security event for network denial events, On** to enable the creation of a security log event when the underlying network firewall denies a network connection.
- **Log security event for network denial events, Off** to disable the creation of a security log event when the underlying network firewall denies a network connection.

- Click **Help** to display help for the current window.

Security Logs table

When you open a security log, the window lists the most recent (latest) security events. The events are listed in order of occurrence (from the most recent event to the oldest event). Only a subset of the events is listed; click **Show Earlier Events** or **Show Later Events** to navigate to other subsets of events.

User
Displays the user ID from which the security event occurred.

Date
Displays the date and time the event occurred.

Security Event
Displays a description of the event.

Additional information is available for events marked with an asterisk (*). Click **Details...** to display the information.

Additionally, you can perform the following actions from the table:

Details...
To display additional information about a selected event, click **Details...**. The Security Log Details window is displayed. To close the window, click **OK**.

Authentication Data...
To display authentication data for the selected event, click **Authentication Data...**. The Authentication Data window is displayed. To close the window, click **OK**.

Show Earlier Events
To display events that occurred *before* the events currently displayed (use it to navigate to older events in the security log), click **Show Earlier Events**.

Note: This option is available only when earlier events are available. Otherwise, it is unavailable.

Show Later Events
To display events that occurred *after* the events currently displayed (use it to navigate to more recent events in the security log), click **Show Later Events**.

Note: This option is available only when later events are available. Otherwise, it is unavailable.

Retrieve from Removable Media or FTP Server

Use this window to open a security log from a USB flash memory drive or from an FTP server.

Hardware Management Console USB flash memory drive
To retrieve a security log from a Hardware Management Console USB flash memory drive, select **Hardware Management Console USB flash memory drive**. A table is displayed which includes the available USB flash memory drives. To make sure you have the available USB flash memory drive, click **Refresh**.

Note: If you're using a USB flash memory drive, plug it into the console. If it is properly inserted, the console beeps three times (if an internal speaker is available and is not muted) and a message is displayed indicating the drive was successfully added. The device is ready and can be accessed. Otherwise, the console will not beep three times and a message may display indicating the drive was not added and that you should remove the device and try again.

FTP Server
To retrieve a security log from an FTP server, select **FTP Server**. The following input areas are displayed.

Host name:
Specify the host name address or destination. This is a required field.

User name:
Specify the user name for the target FTP destination. This is a required field.

Password:
Specify the password that is associated with the user name for the target FTP destination. This is a required field.

Protocol:

Choose a secure network protocol for transferring files.

- **FTP** (File Transfer Protocol) - This is the default.
- **FTPS** (FTP Secure)
- **SFTP** (SSH File Transfer Protocol)

File path
When you have selected either a USB flash memory drive or an FTP server the security log is to be saved to, you must provide the path name in the input area or click **Browse**. Once you make your directory selection it is displayed in the input area.

If you do not provide a file path for a USB flash memory drive, then the default is to the media mount point. If you do not provide a file path for an FTP selection, then the default is to the home directory of the FTP server.

Note: The file path has a maximum length of 2048 characters.

OK
To proceed with your selection, click **OK**.

Cancel
To exit this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Search by Date

Use this window to set a time and date for locating events in the security log that are currently open:

1. Use the **Desired Time** field to set the time. Specify the hours, minutes, and seconds (hh:mm:ss.SSS). Initially, the current time appears in this field.
2. Use the **Desired Date** field to set the date. Specify the month, day, and year (mm/dd/yyyy). Initially, the current date appears in this field.
3. Click **Find Event** to begin the search.

The search begins with the first event in the log and proceeds in order of event occurrence (from the most recent event to the oldest event).

Upon locating events that occurred at or before the specified desired time and date, the **View Security Logs** window is displayed again with the events listed in order of occurrence.

Additionally, the Search by Date window includes the following:

Newest Time
Specifies the time of the most recent security log in the list.

Oldest Time
Specifies the time of the oldest security log in the list.

Newest Date
Specifies the date of the most recent security log in the list.

Oldest Date
Specifies the date of the oldest security log in the list.

Cancel
Exit this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Search by Event

Use this window to select an event description to search for in the security log currently open:

1. Select an event description from the list.
2. Click **OK** to display the list of security logs matching the selected event type.

   The view security logs window is displayed again with the matching events.

   Note: The **Find Earlier Event** and **Find Later Event** options are disabled if there are fewer than 500 events.

Event description list
This list displays the security log event descriptions that you can select. When an event is selected (highlighted), click **Find Earlier Event** or **Find Later Event** to search for the next event. The sorting of the events depends on which option you selected.

Find Earlier Event
To search the security log for an event that is older than the currently displayed events, click **Find Earlier Event**.

Find Later Event
To search the security log for an event that is more recent than the currently displayed events, click **Find Later Event**.

Full Text
To view the entire event description, select the event, then click **Full Text**.

The **Full Text of Security Event** window is displayed, click **OK** when you are done viewing the window.

Cancel
To exit this window without saving any changes, click **Cancel**.

Help
To display help for the current window, click **Help**.

Search By Event Categories

Use this window to select the subset of security events (defined by the appropriate category) you want to view.

OK
After selecting a category, click **OK** to view the security logs that pertain to that category.

Cancel
To exit this window, click **Cancel**.

Category Content
To determine which events are in a selected category, click **Category Content**.

The **Category Content** window is displayed, click **OK** when you are done viewing this window.

Help
To display help for the current window, click **Help**.

Search by User Name

Use this window to provide a user ID that is associated with the events you want to view.

User
Specify a user name in the text input area.

OK
To proceed with the user ID you have entered, click **OK**.

Cancel
To return to the previous window without searching for a specified user ID, click **Cancel**.

Help
To display help for the current window, click **Help**.

View Service History

Accessing the Perform Problem Analysis task

The Support Element starts Problem Analysis automatically only upon detecting a problem. While the Support Element provides very comprehensive error detection, if it does not detect a problem you suspect is affecting the system or Support Element, you can use the Support Element workplace to start Problem Analysis manually.

To start Problem Analysis manually:

1. Locate the system to work with.
2. Open the **Perform Problem Analysis** task.
3. Use the Perform Problem Analysis window to start Problem Analysis manually.

   Problem Analysis will issue a hardware message to notify you if it identifies a problem.
4. Click **View All Errors...** to view details on all error in the display list.
5. Click **View Selected Errors...** to view details on a selected error in the display list.
6. Click **Cancel** to exit the window.

Accessing the View Service History task

You can use the Support Element workplace to display the service history of the system. This task displays a list of current problems for the system. The problems may be opened or closed with the most recent entry at the top of the list.

To display the service history:

1. Locate the system to work with.
2. From the menu bar you can:
   - Select **View** for the following choices:

     Problem Summary
     Displays detailed information about the selected problem including machine type, model, and serial number information.

     Problem Analysis Panels
     Redisplays the Problem Analysis (PA) windows that were created when the selected problem was originally reported.

     Repair Information
     Displays repair information for the selected problem.

     Exit
     Ends the task.
   - Select **Close** for the following choices:

     Selected Problem
     Changes the current status of the selected problem to closed.

     All Problems
     Changes the current status of all open problems to closed.

- Select **Sort** for the following choices:

  By Date
  Lists problems in the order of the dates on which problems occurred, starting with the most recent problem.

  By System Name
  Lists problems by the alphabetical order of the names of the objects on which they occurred.

  By Status
  Lists all open problems, followed by all closed problems.
- Select **Help** to display additional task information.

3. When you have completed this task, select **View**, **Exit**.

Service History

Use this window to review or close problems discovered by Problem Analysis, or reported using Problem Analysis, for one or more objects.

A problem is *opened* when either:

- Problem Analysis determines service is required to correct a problem detected by the object
- A console operator uses the **Report a Problem** task to report a suspected problem not detected by the object.

Each record of a problem includes detailed information about the problem, and indicates whether the service required to correct the problem is still pending (an *opened* problem), or is already completed or no longer needed (a *closed* problem).

Collectively, the problem and service records are referred to as the *service history* of the object. Upon viewing the object's service history, you can:

- Redisplay the Problem Analysis windows that were displayed when a problem was originally reported.
- Display detailed information about a problem.
- Manually close open problems.

Click **View** on the menu bar, then select the following:

- **Problem Summary...** to display additional information that further describes the selected problem and the object it occurred on, and lists actions performed to diagnose and correct the problem.
- **Problem Analysis Panels...** to display Problem Analysis panels that were shown to report the selected problem when it occurred.
- **Repair Information...** to display the repair information for the selected problem.
- **Exit** to end this task and return to the console workplace.

Click **Close** on the menu bar, then select the following:

- **Selected Problem** to change the status of selected *open* problems to *closed*.
- **All Problems** to change the status of all *open* problems to *closed*.

Click **Sort** on the menu bar, then select the following:

- **By Date** to list problems in order of the dates on which they occurred, from the most recent problem to the oldest problem.
- **By System Name** to list problems in alphabetical order of the names of the objects on which they occurred.
- **By Status** to list all *open* problems, followed by all *closed* problems.

Click **Help** to display help for the current window.

Service History table

This list displays the most recent problems that were automatically detected by Problem Analysis, or reported manually using Problem Analysis, for all selected objects.

Date
Displays the date on which the problem occurred.

Time
Displays the time when the problem occurred.

System name
Displays the name of the object on which the problem occurred.

Problem Number
Displays the number assigned by Problem Analysis and used to identify and track the problem.

Status
Indicates whether the problem is *open* or *closed*.

Description
Displays a brief explanation of the problem.

Service History Problem State

This window displays information that identifies an object, describes a specific problem that occurred on it, and lists actions performed to diagnose and correct the problem.

System name
Displays the name of the object on which the problem occurred.

Machine type
Displays the machine type of the object.

Machine model
Displays the model number of the object.

Machine serial number
Displays the serial number of the object.

Remote support problem number
Displays the remote support problem number.

Problem number
Displays the number assigned to the problem by Problem Analysis.

Problem type
Identifies the type of problem reported to the support system by Problem Analysis, and indicates the type of service required to correct it.

Problem data
Displays additional information provided by Problem Analysis specifically for this problem.

The information may be part numbers of parts needed to repair the problem, or reference codes needed to perform additional problem determination.

Problem State table

Date
Displays the date on which the problem occurred.

Time
Displays the time when the problem occurred.

“Problem States” on page 978
Displays the problem state of the object on which the problem occurred.

Problem States

Descriptions of the problem states or their effects on the problem:

Additional problem information
Indicates a service representative, while performing a repair procedure, manually edited the service history log to further describe the problem or its repair.

Continued in printed information
Indicates a repair procedure instructed a service representative to continue the repair using a printed repair procedure.

Customer notified
Indicates Problem Analysis displayed a panel to report the problem.

Duplicate problem closed
Indicates Problem Analysis closed the problem because it was a duplicate of another open problem.

Inactive problem closed
Indicates Service History closed the problem because of inactivity.

Problem closed
Indicates Problem Analysis could no longer detect the problem after a service representative completed a repair procedure.

Problem closed by the user
Indicates the console operator used the Service History task to close the problem.

Problem detected
Indicates Problem Analysis detected the problem automatically.

Problem reopened
Indicates Problem Analysis detected the problem occurred again after it was repaired and closed.

Repair closed
Indicates a problem was closed when the repair was completed.

Repair ended
Indicates a service representative completed a repair procedure.

Repair resumed
Indicates a service representative started using a previously suspended repair procedure.

Repair started
Indicates a service representative began a repair procedure.

Repair suspended
Indicates a service representative temporarily stopped using a repair procedure before completing the repair.

Returned from printed information
Indicates a service representative resumed using a repair procedure to acknowledge completing a printed repair procedure.

Service authorization complete
Indicates Problem Analysis successfully transmitted problem information and requested service through a Remote Support Facility (RSF) connection to the support system.

Service authorization delayed
Indicates Problem Analysis reported the problem, but the console operator did not request service.

Service authorization failed
Indicates Problem Analysis could not successfully transmit problem information or request service through a Remote Support Facility (RSF) connection to the support system.

Service authorized electronically
Indicates Problem Analysis used the Remote Support Facility (RSF) to connect to the support system to transmit problem information and request service.

Service requested via telephone
Indicates Problem Analysis displayed problem information and instructed the console operator to call a service representative, describe the problem, and request service.

Additional functions are available from this window:

OK

To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Help
To display help for the current window, click **Help**.

Service History Part Replacement

This window displays part replacement information including part descriptions as well as how many parts were replaced.

Part Location
Displays the machine location of the object on which the problem occurred.

Part Number
Displays the actual part number of the object.

Serial Number
Displays the serial number of the object.

Fix description
The description from Service History of how to correct the problem.

OK

to return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Help
To display help for the current window, click **Help**.

Problem Analysis (problem description)

This window displays the following information about a problem discovered by automatic Problem Analysis:

System name
Displays the name of the object on which the problem occurred.

Date
Displays the date on which the problem occurred.

Time
Displays the time when the problem occurred.

Depending on the information that was provided for a problem, the following information could also appear in this window:

Channel path
Displays a four-digit physical channel identifer (PCHID) of the channel on which the error occurred, for example: 0131, 0132, or 0133.

Unit address
Displays the address of the device the channel path was being used to communicate with when, or immediately before, the Interface Control Code (IFCC) occurred.

Tag-in control lines
Displays a two-digit, hexadecimal value that identifies the inbound tags that were active when the IFCC occurred.

Tag-out control lines
Displays a two-digit, hexadecimal value that identifies the outbound tags that were active when the IFCC occurred.

Bus-in data lines
Displays the value on the inbound data lines when the IFCC occurred.

Bus-out data lines
Displays the value on the outbound data lines when the IFCC occurred.

Use the following information to determine whether to request service, then take the appropriate action:

Problem Description
Provides a brief description of the problem.

Corrective Actions
Describes what actions an operator can take to correct the problem.

Impact of Repair
Describes what system resources will be affected.

Additional functions are available from this window:

Request Service...
To request service to correct the problem, click **Request Service...**.

I/O Trace...
To display Input/Output (I/O) trace information, click **I/O Trace...**.

No Service
To handle the problem without requesting service, click **No Service**.

Display Service Information...
To display information about an automatic Problem Analysis operation on an object, click **Display Service Information...**.

Display Sense Data
To display additional specific problem failure information, click **Display Sense Data**.

Detail Problem Description...
To view a more detailed description of the problem, click **Detail Problem Description...**.

Delete
To delete from **Hardware Messages** the message you selected to display this window, and to close this window, click **Delete**.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Tag-in control lines

This field displays a two-digit, hexadecimal value that identifies the inbound tags that were active when an interface control check (IFCC) occurred.

The hexadecimal number represents the values of eight bits:

- The first digit of the hexadecimal number represents the values for bits 0 through 3.
- The second digit of the hexadecimal number represents the values for bits 4 through 7.
- The value for a bit is 1 when its tag-in is active.

- The value for a bit is 0 when its tag-in is not active.

Bit	Tag-In
0	Operational
1	Address
2	Status
3	Select
4	Request
5	Service or Data (see Note)
6	Data or Mark (see Note)
7	Disconnect

Note: The values for bits 5 and 6 indicate whether the following tags-in are active:

```
Bit 5    Bit 6          Data In       Service       Mark
-----    -----          -------       -------       ----
 1        1              On            Off           Off
 1        0              Off           On            Off
 0        1              Off           Off           On
 0        0              Off           Off           Off
```

For example, a tag-in value of 86 indicates that Operational In and Data In are both active.

Tag-out control lines

This field displays a two-digit, hexadecimal value that identifies the outbound tags that were active when an interface control check (IFCC) occurred.

The hexadecimal number represents the values of eight bits:

- The first digit of the hexadecimal number represents the values for bits 0 through 3.
- The second digit of the hexadecimal number represents the values for bits 4 through 7.
- The value for a bit is 1 when its tag-out is active.
- The value for a bit is 0 when its tag-out is not active.

Bit	Tag-In
0	Operational
1	Address
2	Select/Hold
3	Data streaming
4	Service
5	Data
6	Suppress
7	Command

For example, a tag-out value of 84 indicates that Operational Out and Data Out are both active.

Problem Analysis (sense data details)

This window displays sense data details and additional problem failure information.

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Help
To display help for the current window, click **Help**.

Problem Analysis (operation/outcome)

This window displays information about an automatic Problem Analysis operation on an object. The information identifies the operation and describes its outcome.

Review the information, then take the appropriate action.

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Delete Message
To delete from **Hardware Messages** the message you selected to display this window, and to close this window, click **Delete Message**.

Cancel
To close this window and keep the message, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (problem information)

This window displays information about a problem discovered by automatic Problem Analysis.

Use the information provided to determine whether to request service, then take the appropriate action.

System name
Displays the name of the object that had the channel path configured on when the IFCC occurred.

Channel path
Displays a four-digit physical channel identifier (PCHID) of the channel on which the error occurred, for example: 0131, 0132, or 0133.

Unit address
Displays the address of the device the channel path was being used to communicate with when, or immediately before, the IFCC occurred.

Tag-in control lines
Displays a two-digit, hexadecimal value that identifies the inbound tags that were active when the IFCC occurred.

Tag-out control lines
Displays a two-digit, hexadecimal value that identifies the outbound tags that were active when the IFCC occurred.

Bus-in data lines
Displays the value on the inbound data lines when the IFCC occurred.

Bus-out data lines
Displays the value on the outbound data lines when the IFCC occurred.

Additional functions are available from this window:

Problem Description
Provides a brief description of the problem.

Corrective Actions
Describes what actions an operator can take to correct the problem.

Request Service...
To request service to correct the problem, click **Request Service...**.

No Service
To handle the problem without requesting service, click **No Service**.

Display Service Information...
To display information about an automatic Problem Analysis operation on an object, click **Display Service Information...**.

Delete Message
To delete from **Hardware Messages** the message you selected to display this window, and to close this window, click **Delete Message**.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (contact)

Use this window to identify a person that can be contacted about the problem, and to specify how to service will be requested.

Provide the following information, then click **Request Service...**:

Customer name
Specify the name of the person that can be contacted about the problem.

Customer phone
Specify the telephone number of the person that can be contacted about the problem.

Transmission Type
Select how to request service, through automatic transmission or manually by telephone.

Select a transmission type, then click **Request Service...**.

Electronic transmission
To automatically transmit the service request and problem information, select **Electronic transmission**.

Voice transmission
To manually request service and report problem information by telephone, select **Voice transmission**.

Note: The telephone number and problem information are provided on a subsequent window.

Additional functions are available from this window:

Request Service...
To authorize service for this problem and initiate the transmission type by electronic or by voice, select click **Request Service...**.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (problem information/contact)

This window displays information about a problem discovered by automatic Problem Analysis. Use this information to request service and describe the problem.

1. Be ready to provide the problem information when you call.
2. Dial the telephone number to speak with a service representative.
3. Request service.
4. Provide the problem information to the service representative.

Request service when:

- Service is required.
- Service may be required, and you have verified all possible causes of the problem do not exist.

It is recommended you do not request service when:

- Service is not required.
- Service may be required, but you have verified one or more possible causes of the problem exist, and you will attempt to correct the problem.

Additional functions are available from this window:

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (action to take)

This window displays information about a problem discovered by automatic Problem Analysis.

Review the information, then take the appropriate action.

Problem Data
Provides specific information about the selected problem.

Parts List

- Part Location - the physical location of the part.
- Part Number - the number of the part.
- Fix Percentage - the percentage of accuracy for correcting the problem.
- Serial Number - the serial number of the part.
- Quantity - the number of parts.

Additional functions are available from this window:

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Delete Message
To delete from **Hardware Messages** the message you selected to display this window, and to close this window, click **Delete Message**.

Cancel
To close this window and keep the message, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (trace information)

This window displays the following interface trace information:

Function
Whenever possible, a description of the operation being performed for each tag displayed and bus sequence is shown under this field; Interface Disconnect, Interface Control Check (IFCC), Recovery-Hung Interface, etc.

In Tags
Indicates the state of each inbound tag. A plus (+) below the line indicates an active state of the line. A period (.) indicates the inactive state of the line.

REQ
Displays the Request In tag line. This raised by a control unit to indicate it needs service to present status or to perform a data transfer operation.

SEL
Displays the Select In tag line. This is the return of Select Out that indicates no control unit captured the Select Out signal.

OP
Displays the Operational In tag line. This normally indicates the selection of a control unit by the channel.

ADR
Displays the Address In tag line. This defines the information on the Bus In lines as the address of the currently selected I/O device.

STA
Displays the Status In tag line. This defines the information on the Bus In lines as status information.

SRV
Displays the Service In tag line. This defines the information on the Bus In lines as data for a read operation. For a write operation, this indicates a control unit request for data.

DAT
Displays the Data In tag line. This defines the information on the Bus In lines as data for a read operation. For a write operation, this signals a request for data.

DIS
Displays the Disconnect In tag line. This signals a control-unit-detected problem.

MKO
Displays the Mark In 0 line. This is used primarily with the bus extension feature to tell the channel that it is working with a reliable control unit.

Bus In
Indicates the hexadecimal value on the Bus In lines.

Out Tags
Indicates the state of each outbound Tag. A plus (+) below the line indicates an active state of the line. A period (.) indicates the inactive state of the line.

OP
Displays the Operational Out tag line. This is used for interlocking. All outbound tag lines except for Suppress Out are significant only as long as this line is active.

ADR
Displays the Address Out tag line. This defines the information on the Bus Out lines as a device address.

SEL
Displays the Select Out tag line. This captured by a control unit or device waiting to operate with the channel. Capturing Select Out and then Raising Operational In begins the connection process.

CMD
Displays the Command Out tag line. This indicates to stop, proceed, stack status, or identify Bus Out data.

SRV
Displays the Service Out tag line. This defines the information on the Bus Out lines as data for a write operation. For a read operation, this indicates the channel accepted the data. In reply to Status In, this indicates the acceptance of status.

DAT
Displays the Data Out tag line. This defines the information on the Bus Out lines as data.

SUP
Displays the Suppress Out tag line. This is used alone or with other lines to:

- Indicate command chaining
- Force status suppression
- Perform a selective reset
- Force data suppression.

Bus Out
Indicates the hexadecimal value on the Bus Out lines.

Elapsed Time (us)
This field contains elapsed time count data. During critical points of the input/output trace, this count data is reset and the field will contain a line of dashes. The next line entry after this reset will contain the elapsed time from the reset state in microseconds, until that interface operation completes. As each interface sequence occurs, its elapsed completion time will add to the running total until the counter is reset again.

Additional functions are available from this window:

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Help
To display help for the current window, click **Help**.

Problem Analysis (ESCON trace information)

This window displays the following ESCON interface trace information:

- **Function** - the function name
- **UA** - the unit address
- **CCW** - Channel Command Word
- **Flg** - Flags
- **Sta** - Status
- **Other fields** - additional fields
- **Time** - the relative time stamp used for comparison
- **Log Data** - additional data.

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Help
To display help for the current window, click **Help**.

Problem Analysis (I/O trace information)

This window displays the following Input/Output (I/O) interface trace information:

In Tags
Indicates the state of each inbound tag. A plus (+) below the line indicates an active state of the line. A period (.) indicates the inactive state of the line.

REQ
Displays the Request In tag line. This raised by a control unit to indicate it needs service to present status or to perform a data transfer operation.

SEL
Displays the Select In tag line. This is the return of Select Out that indicates no control unit captured the Select Out signal.

OP
Displays the Operational In tag line. This normally indicates the selection of a control unit by the channel.

ADR
Displays the Address In tag line. This defines the information on the Bus In lines as the address of the currently selected I/O device.

STA
Displays the Status In tag line. This defines the information on the Bus In lines as status information.

SRV
Displays the Service In tag line. This defines the information on the Bus In lines as data for a read operation. For a write operation, this indicates a control unit request for data.

DAT
Displays the Data In tag line. This defines the information on the Bus In lines as data for a read operation. For a write operation, this signals a request for data.

DIS
Displays the Disconnect In tag line. This signals a control-unit-detected problem.

MKO
Displays the Mark In 0 line. This is used primarily with the bus extension feature to tell the channel that it is working with a reliable control unit.

Bus In
Indicates the hexadecimal value on the Bus In lines.

Out Tags
Indicates the state of each outbound Tag. A plus (+) below the line indicates an active state of the line. A period (.) indicates the inactive state of the line.

OP
Displays the Operational Out tag line. This is used for interlocking. All outbound tag lines except for Suppress Out are significant only as long as this line is active.

ADR
Displays the Address Out tag line. This defines the information on the Bus Out lines as a device address.

SEL
Displays the Select Out tag line. This captured by a control unit or device waiting to operate with the channel. Capturing Select Out and then Raising Operational In begins the connection process.

CMD
Displays the Command Out tag line. This indicates to stop, proceed, stack status, or identify Bus Out data.

SRV
Displays the Service Out tag line. This defines the information on the Bus Out lines as data for a write operation. For a read operation, this indicates the channel accepted the data. In reply to Status In, this indicates the acceptance of status.

DAT
Displays the Data Out tag line. This defines the information on the Bus Out lines as data.

SUP
Displays the Suppress Out tag line. This is used alone or with other lines to:

- Indicate command chaining
- Force status suppression
- Perform a selective reset
- Force data suppression.

Bus Out
Indicates the hexadecimal value on the Bus Out lines.

Misc
Indicated the state of the non-interface type lines defined by flags. A plus (+) below the line indicates an active state of the line. A period (.) indicates the inactive state of the line.

ACT
Displays the I/O interface active flag. This flag indicates that the I/O interface is active. The interface is considered active when select-out is active. The interface is considered inactive when select-out is inactive, when all bus-in signals are inactive (including bus-in-p), and when all tag-in signals are inactive (except request-in).

DX
Displays the parallel data transfer mode flag. This flag is active during a data transfer operation.

SGV
Displays the stop given flag. A PARDX command out was issued.

ICC
Displays the interface control check error flag.

Elapsed Time (us)
This field contains elapsed time count data. During critical points of the input/output trace, this count data is reset and the field will contain a line of dashes. The next line entry after this reset will contain the elapsed time from the reset state in microseconds, until that interface operation completes. As each interface sequence occurs, its elapsed completion time will add to the running total until the counter is reset again.

Additional functions are available from this window:

OK
To return to the previous window when you have finished reviewing the displayed information, click **OK**.

Note: Problem Analysis will send hardware messages to report new information about the problem and your service request. Use the **Hardware Messages** task with the selected system to display the new information.

Help
To display help for the current window, click **Help**.

Problem Analysis (channel path errors)

This window displays the unreported errors that occurred on a specific channel path of a Central Processor Complex (CPC).

Use this window to select an error when you want to display detailed information from Problem Analysis that describes the error.

Select one error from the list, then click **Analyze Error...** to display details about the error.

System name
Displays the name of the CPC that had the channel path configured on when the error occurred.

Channel path
Displays a four-digit physical channel identifier (PCHID) of the channel on which the error occurred, for example: 0131, 0132, or 0133.

Interface location
Identifies the physical location of the channel card and port that supports the channel path on which the error occurred.

Additional functions are available from this window:

Error table

Date
Displays the date the error occurred.

Time
Displays the time the error occurred.

Description
Displays a brief description of the error.

Analyze Error...
Select an error from the list, then click **Analyze Error...** to display details about the selected error.

Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Problem Analysis (unreported errors)

This window summarizes the unreported errors that occurred on the system. The summary identifies the problem areas where errors occurred, and displays the number of errors that occurred in each area.

Use this window to select a problem area when you want to display more information about the unreported errors that occurred in the area.

Problem areas for a CPC include the processors and its channels paths.

An unreported error is an error that is analyzed, but is not reported by Problem Analysis. Errors are not reported when automatic recovery operations succeed, and when service is not needed for the system to continue operating.

Select a problem area for a system from the list, then click **View Selected Errors...** to display a summary of unreported errors that occurred in that area.Or, you can click **View All Errors...** to display a listing of all the processor and channel errors sorted by **Date Time** within the **Problem Area**.

Beginning time
Displays the time and date when the least recent unreported error occurred.

All unreported errors occurred at or after this time.

Ending time
Displays the time and date when the most recent unreported error occurred.

All unreported errors occurred before or at this time.

Error table

System Name
Displays the name of the system where the unreported errors occurred.

Problem Area
Indicates whether the unreported errors occurred on a processor in the CPC, or on a particular channel path.

Number of Errors
Indicates the number of unreported errors that occurred in the problem area during the time range.

View All Errors...
To view details about all errors shown in the list, click **View All Errors...**.

View Selected Errors...
To view details about one error in the list, click **View Selected Errors...**.

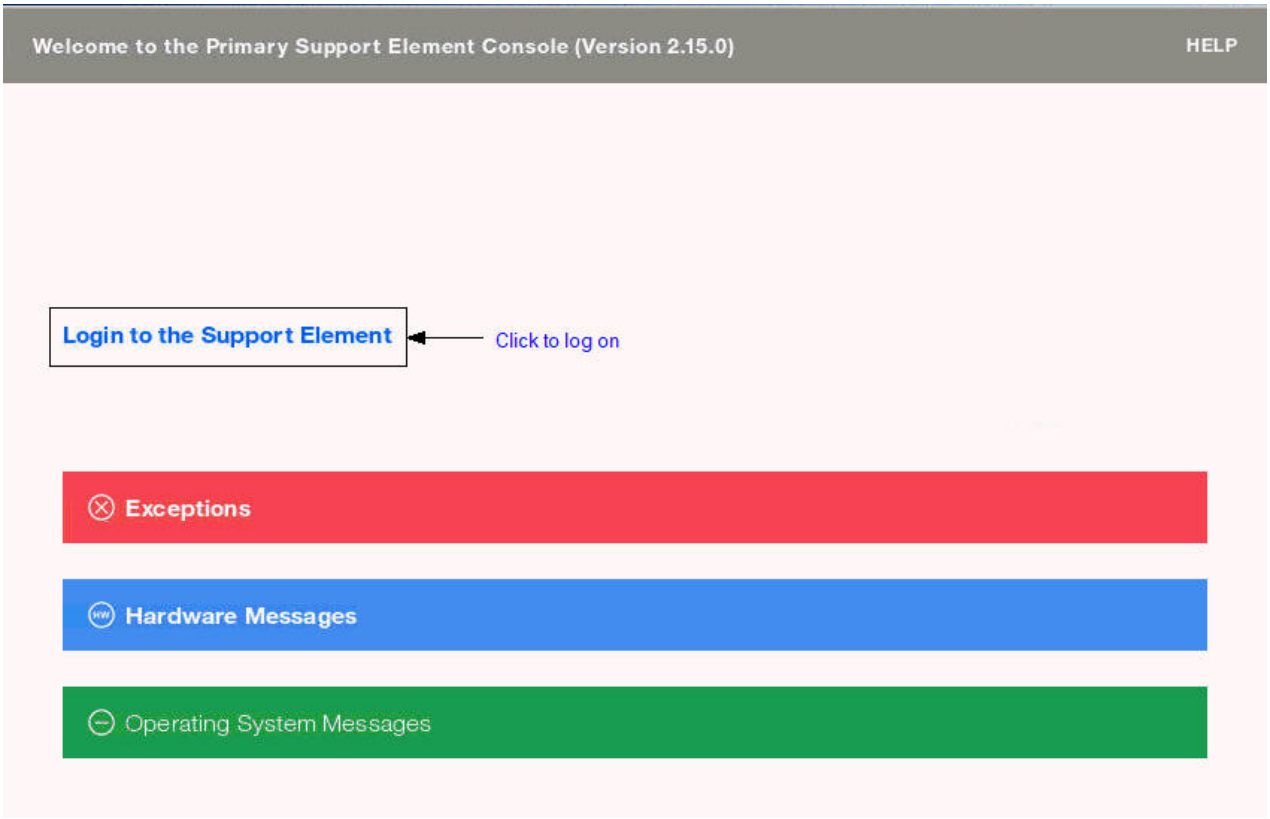
Cancel
To not allow service at this time, or to close this window without requesting service, click **Cancel**.

Help
To display help for the current window, click **Help**.

Welcome

Welcome to the Support Element

Use this window to log on and start the console and see an overview of the system status.



The elements of this window allow you to do the following:

- View the online help
- Learn the status of the console

Log On

To log on to the console, select the **Login to the Support Element** link.

This takes you to the logon window where you provide your user ID and password.

Online Help

To view the online help for the console, click **HELP** found in the upper right corner of the window.

Status overview

The status overview area of this window indicates the system status of the objects.

Exceptions

When no objects exist with unacceptable status, then the **Exceptions** bar is green to convey a positive status. If there are objects that have exceptions, then the bar is red. To view the exceptions and log on to the Support Element, select the **Exceptions** link.

Hardware Messages

When no objects exist with hardware messages, then the **Hardware Messages** bar is green to convey a positive status. If there are objects that exist with hardware messages, then the bar is blue. To view the hardware messages and log on to the Support Element, select the **Hardware Messages** link.

Operating System Messages

When no objects exist with operating system messages, then the **Operating System Messages** bar is green to convey a positive status. If there are objects that exist with operating system messages, then the bar is purple. To view the operating system messages and log on to the Support Element, select the **Operating System Messages** link.

Index

A

about 484
accessibility
  contact IBM 269
  features 269, 270
accessing
  release I/O path 785
  view licenses task 967
accessing manage adapter firmware 660
account information task
  instructions for starting 442
account information, about 442
activate task
  instructions for starting 301
activation profiles
  about 483
  customizing 483
  default profiles 483, 484
  image profiles, customizing 506
  load profiles, customizing 508
  types of 484
  types to use, choosing the right 484
adapter details 306
add a feature, perform model conversion 756
adding logical processors 648
addressing mode, display or alter 551, 553
advanced facilities 309
alternate support element
  querying switch capabilities between support elements 341
alternate Support Element 339
analyze internal code task 344
API settings, customizing 444
application programming interface
  enabling 444
assigning domain security 556
assistive technologies 269
audit and log management task
  audit report 350
  log report 350
audit report 350
authorize concurrent internal code changes task
  instructions for starting 779
authorize internal code changes task
  instructions for starting 350
automatic activation, about 352
automatic activation, aboutCPC operational customization task list, instructions for starting tasks in
  automatic activation 352
  automatic activation task
    instructions for starting 352
automatic licensed internal code change installation
  blocking 354

B

block automatic licensed internal code change installation task 354
blocking automatic licensed internal code change installation 354
broadcast message 419
broadcast messages 450
browser
  remote power off or restart 450
build data set, input/output configuration 620

C

central processor complex
  activating 301
  deactivating 545
  load image, performing manually for error recovery 640
  reset normal of image, performing for daily operation 794
change identifier 578
change internal code task 355
change logical partition group controls task 385
Change Logical Partition Security 392
change LPAR controls 375
change LPAR controls task
  instructions for starting 375
change lpar input/output priority queuing task 388
change LPAR security 392
change LPAR security task 392
change management
  operating system messages 691
change management task list, instructions for starting tasks in
  authorize concurrent internal code changes 779
  authorize internal code changes 350
  system information 852
change mirror time task 397
change password task 398
changing group controls,logical partition 385
changing logical partition cryptographic controls 382
changing LPAR I/O priority queuing 388
changing password task 397
channel details 398
channel information, displaying 404
Channel location to PCHID assignment 403
channel operations task list, instructions for starting tasks in
  advanced facilities 309
channel path configuration, input/output configuration 621
channel paths 404
channel problem determination 404, 405
channel problem determination task, instructions for starting 404
channel problem determination task, instructions for starting in 405

channel subsystem information, input/output configuration 624
channel subsystem selection, input/output configuration 624
channel to PCHID assignment 402
Channel to PCHID Assignment 402
check held LIC changes during install 450
checking dependencies 405
checking redundant I/O multiport status 784
checkout tests task
  instructions for starting 411
checkout tests, about 411
Choose a Disconnected Session 412
CHPID information, input/output configuration 627
CHPID operations task list, instructions for starting tasks in
  reassign I/O path 781
  release 786
  service on/off 801, 811
CHPIDs
  reassigning reconfigurable 781
clonable internal code levels 546
concurrent processor drawer replacement 742
configuration
  operating system messages 691
configuration tasks
  system input/output configuration analyzer 860
  transmit vital product data 869
  view frame layout 962
Configure On/Off 413
configuring on/off task 413
confirmations 416, 934
console actions
  audit and log management 348
  block automatic licensed internal code change installation 354
  change password 397
  console messenger 418
  customize console services 449
  customize network settings 454
  customize user controls 897
  logoff or disconnect 652
  manage print screen files 666
  manage remote support requests 670
  perform a repair action 735
  power off or restart 772
  rebuild vital product data 783
  save upgrade data 795
  save/restore customizable console data 796
  user management 873
  users and tasks 936
  view console events 959
  view licenses 967
console actions work area, instructions for starting actions in
  customize date/time 482
  logoff 10
console messenger 450
console messenger task
  broadcast message 419
console tasks
  audit and log management 348
  authorize internal code changes 351
  change internal code 355
console tasks *(continued)*
  change password 398
  customize network settings 455
  manage print screen files 667
  network diagnostic information 680
  power off or restart 772
  rebuild vital product data 783
  save upgrade data 796
  users and tasks 937
console, Support Element from a hardware management console 9
control unit header, displaying 404
control unit information, input/output configuration 628
copy configuration, input/output configuration 616
CP Address Match controls 817
CP toolbox task list, instructions for starting tasks in
  interrupt 640
  start 811
  stop 814
CP/SAP Details 423
CPC
  activating 301
  deactivating 545
  power-on reset, performing manually for error recovery 774
  reset normal of image, performing for daily operation 794
cpc configuration
  edit frame layout 564
CPC configuration task list, instructions for starting tasks in
  input/output configuration 612
cpc details 824
CPC operational customization task list, instructions for starting tasks in
  change LPAR controls 375
  customization activation profiles 486
  enable/disable dynamic channel subsystem 491, 580
  scheduled operations 467
  storage allocations, instructions for reviewing current 819
  storage information 819
  storage Information task 819
  view LPAR cryptographic controls 505, 967
CPC recovery task list, instructions for starting tasks in
  power-on reset 775
  power-on reset, performing manually for error recovery 774
  reset clear 794
CPC recovery task list, instructions for stopping tasks in 817
cryptographic configuration 424
cryptographic controls for logical partitions
  customizing in activation profiles 504
  viewing 505, 967
Cryptographic Management 440
current program status word (psw), display or alter 552
Customer Information task 442
customize
  API settings task 444
  user controls task 897
customize API settings 444
customize console services task
  check held LIC changes during install 450
  console messenger 450
  remote power off or restart 450

customize date/time console action
instructions for starting 482
customize network settings task 455
Customize Product Engineering Access 465
Customize Remote Service 788
customize support element date/time task 482
customize/delete activation profiles
task
instructions for starting 506
customizing network settings task
console actions 454

D

daily task list
activate 301
deactivate 545
reset normal 795
daily tasks
operating system messages 691
deactivate 545
deactivate task
instructions for starting 545
deactivation 545
define clonable internal code level 546
defining clonable internal code levels 546
delete LPAR dump data task
instructions for starting 547
device information, input/output configuration 629
device status, displaying 404
disable write protection, input/output configuration 616
disabling
check help MCLs during install 450
console messenger 450
console services
check held MCLs during install 450
remote power off or restart 450
remote power off or restart 450
disassemble data set, input/output configuration 621
display assigned port names 590
display FCP NPIV port names 590
display or alter
instructions for starting 550
display or alter, register entry fields 551
display or alter, selected cp 551
display or alter, storage entry fields 553
Display Processor Upgrade Data 746
displaying the infiniband adapter ID task 549
disruptive tasks 13
domain security task 556
domain security, assigning 556
dump coupling facility logical partition data 560
dump data, about 559, 563
dump LPAR data task
instructions for starting 560
dynamic I/O configuration
about 490
CPC, activating to support using 490
IOCDS, using to select 488
load attributes, using to set 502
logical partition, activating to support using 496
dynamic information, input/output configuration 633

E

eBusiness on Demand 746
Edit Frame Layout 564
edit frame layout task 564
edit internal code change 578
enable I/O priority queuing 579
enable input/output priority queuing 579
enable write protection, input/output configuration 615
enable/disable dynamic channel subsystem task, about 491, 580
enabling
check held LIC changes during install 450
check held MCLs during install 450
console messenger 450
console services
check held LIC changes during install 450
remote power off or restart 450
remote power off or restart 450
enabling automatic Support Element switchover 450
enabling I/O priority queuing 579
enabling NPIV 593
enabling the network message forwarding 450
energy management tasks
set power cap 806
set power saving 809
energy optimization advisor 582
energy optimization task 582
environmental dashboard 584
expand controls 277
export source file, input/output configuration 331, 616, 618
export source file,advanced facilities 338
exporting and importing profile data, instructions for starting task 585

F

FCP configuration 588
FCP NPIV mode 593
force channel internal code update 595
forcibly updating internal code, alternatives 595
forcing channel internal code change 595
format media task 596, 597
function configuration, input/output configuration 631

G

group controls, logical partition 385
group profiles
assigning names
defining group capacity 510

H

hardware messages
about 602
hardware messages task
reporting a hardware problem, instruction for 603
hardware system area token, input/output configuration 633
hipersockets
network traffic analyzer (NTA) 682
HMC management tasks
console messenger 418

I

I/O paths
  reassigning reconfigurable 781
  releasing reconfigurable 785
ICSF 504
image access list, input/output configuration 631
image candidate, input/output configuration 632
image profile
  about 506
  customizing 506
  opening 506
  saving 508
image profile configuration 488
images
  activating 301
  deactivating 545
  operating system messages from, checking 691
IML 775
import source file, input/output configuration 618
infiniband adapter ID,displaying 549
initial microcode load 774
initiating a two-way chat 419
input/output configuration 613
input/output configuration data set
  dynamic I/O, selecting an IOCDS that supports 490
  reset profile, customizing to select for CPC activation 488
input/output configuration program 612
input/output configuration
    task
  instructions for starting 612
installation complete report 635
installation complete report task 635
instant messages 450
instant messaging
  console messenger task 418
  users and tasks task 936
instruction address, display or alter 551, 553
instruction data, display or alter 551
instructions for starting 392, 486
instructions for starting tasks in(manage firmware features 663
instructions for stopping 817
internal code
  keeping records 851
interrupt task
  instructions for starting 640
IOCP 612

K

keyboard
  navigation 269

L

large retrieves from support system 450
LED (light emitting diode)
  setting on 811
licensed internal code, viewing 967
load
  performing manually for error recovery 640
Load From File 645
load from removable media or server task 646
load profile
  about 484
  assigning to CPC 510
  assigning to logical partition 510
  customizing 508
  new, creating 509
  saving 510
load task
  instructions for starting 640
loading software from a removable media or server 645
locking disruptive tasks 13
lockout for disruptive tasks 688
log on 653
log report 350
logical partition cryptographic controls 381
logical partition data, dump 561
logical partition group controls 385
logical partition group name, assigning
  assigning logical partition group name 510
logical processor add task 649
logical processor assignment 374
logically partitioned mode
  activating the CPC in 487
logoff 10
logoff or disconnect task 10, 652
LPAR Internal Code Change Utility 655
LPAR mode
  activating the CPC in 487

M

manage adapter firmware 660
manage adapter firmware, unsupported 663
Manage Enterprise Directory Server Definitions 927
manage firmware features, about 663
manage groups 600
manage print screen files task 667
manage remote support requests task 670
managing groups of objects
  groups, managing 599
managing print screen files task 666
manually setting the Support Element TOD clock 482
memory key, *See* USB flash memory drive
messages
  hardware 603
  operating system 691
mirroring support element to alternate support element 340
monitor tasks
  monitors dashboard 671
monitors dashboard task 671

N

navigation
  keyboard 269
navigation pane collapse 277
network diagnostic information task 680
network diagnostic information, viewing
  console actions
    network diagnostic information 679
  pinging TCP/IP address 679

network settings, customizing 454
network traffic analyzer (NTA) 682
Network Traffic Analyzer Controls 682
new partition advanced task
  attach tape links 717
Nondisruptive Hardware Change 684
NPIV port names, releasing
  releasing NPIV port names 588
NPIV,enabling 593
NTA settings 682

O

object control settings 417, 935
object definition
  operating system messages 691
object locking for disruptive tasks 13
object locking settings task 688
opening 486
operating system messages
  checking 691
  viewing, instructions for 693
operating system messages task
  sending commands, instructions for 693
  viewing messages, instructions for 693
operational customization
  operating system messages 691
operational customization tasks
  change logical partition group controls 385
  change lpar input/output priority queuing 388
  logical processor add 649

P

partition details task
  accessing 694
  add crypto adapters 724
  attach storage groups 716
  boot options 728
  confirm disruptive action dialog 734
  controls 699
  cryptos 720
  general 696
  introduction 694
  memory 703
  network 705
  new hba 719
  new nic 708
  partition links 727
  processors 700
  status 698
  storage 711
  view crypto adapter conflicts 726
  view crypto domain conflicts 727
partition internal code change 578
partition resource assignments
  viewing 969
partitions images configured, input/output configuration 633
password
  changing 397
Password Rules 921
paths to a device, displaying 404
PCI X cryptographic coprocessor feature
  pseudo-random number (PRN) generator 428
pending internal code changes, channels 596
perform a repair action task 735
perform model conversion 739, 740
perform problem analysis task
  instructions for starting 757, 975
performing an alternate support element action 339
pinging the TCP/IP address 679
power off or restart task 772
power-on reset
  performing manually for error recovery 775
Power-on Reset 775
power-on reset task
  instructions for starting 775
power, system
  off, switched automatically during system deactivation 545
  outage, recovery options for automatic system activation after 352
powering off or restarting the system 772
print screen 666
printer to printer, input/output configuration 619
problem determination 404
problems
  check help MCLs during install 450
processor drawer selection table 742
processor running time 374
processor storage
  displaying or altering data 549
product engineering, customizing 465
profiles for complete activation 485, 486
progress
  with multiple targets 864
  with single targets 865
PSW restart
  instructions for starting 779

Q

query coupling facility reactivations 779
query internal code changes pending power-on reset 780
Query Internal Code Changes Pending Power-on Reset 780

R

reassign I/O path 781
reassign I/O path task, instructions for starting 781
rebuild vital product data task 783
recovery
  operating system messages 691
recovery task list, instructions for starting tasks in load 640
redundant I/O multiport status, checking 784
registers, display or alter 551
release I/O path confirmation 786
release I/O path task 786
release subset, NPIV 592
releasing a Crypto Express6S and Crypto Express5S 440
remote customization
  operating system messages 691
remote customization task list, instructions for starting tasks in

remote customization task list, instructions for starting tasks in (continued)
    remote service 787
remote power off or restart 450
remote service task
    instructions for starting 787
remote service, about
    system 787
remove a feature, perform model conversion 756
report a problem task
    instructions for starting 791
reset clear task
    instructions for starting 794
reset normal task
    instructions for starting 795
reset normal, about 794
reset profile
    about 484
    assigning to CPC 487
    navigating the notebook pages 486
    new, creating 487, 507
    opening 486
restarting a processor 779

S

save upgrade data task 795, 796
save/restore customizable console data task 796
saving
    data 796
scheduled operations 466
scheduled operations task
    instructions for starting 467
security settings for logical partitions
    cross partition authority 391, 497
    customizing in activation profiles 496, 497
    global performance data control 391, 496
    input/output configuration control 391, 496
    logical partition isolation 391, 497
    security settings for logical partitions
        customizing in activation profiles 497
select control unit, input/output configuration 625
selecting a crypto type 430
selective channel apply controls 800
Selective Channel Patch Controls 800
sending a message 418
sending messages 450
serial link status, displaying 404
service
    operating system messages 691
    service status 804
    setting on or off 801
Service Channel Path On/Off 801
service data, about 866
service history, about 757, 975
service management
    perform a repair action 735
service management tasks
    installation complete report task 635
    manage remote support requests 670
    rebuild vital product data 783
    view console tasks performed 962
Service On/Off 801
service on/off task (continued)
    instructions for starting 801, 811
Service Required State Query 803
service status task 804
service task list
    checkout tests 411
service task list, instructions for starting tasks in
    checkout tests 411
    delete LPAR dump data 547
    dump LPAR data 560
    perform problem analysis 757, 975
    report a problem 791
    transmit service data 866
    view service history 757, 975
service tasks
    service status 804
services
    customizing
        check held LIC changes during install 450
        remote power off or restart 450
set power cap task 806
set power saving task 809
setting defined capacity 500
setting group capacity
    logical partition group capacity 511
setting the system time offset 495
setting up
    check held LIC changes during install 450
    console messenger 450
    remote power off or restart 450
setting workload manager controls 494
settings for remote connections and communication, tasks for customizing 787
shortcut keys 269
start all 814
start all task
    instructions for starting 814
start task
    instructions for starting 811
stop all 817
stop all task 817
stop on processor CP address match
    instructions for starting 817
stop task
    instructions for starting 814
stopping CPs
    CPs
        stopping 817
Storage Information 819
storage, about 819
storage, display or alter 552
store status
    instructions for starting 823
subchannel data, displaying 404
Support Element Console
    from a Hardware Management Console 8
Support Element Console Application
    starting 8
support element console settings
    customize API settings task 444
support system
    large retrieves 450
supported I/O mask, input/output configuration 634
swap channel path task 823

switching to the alternate Support Element 339
system
  hardware messages from, checking 602
  resetting 794
  settings for system operations, tasks for customizing 483
  shutting down 545
system configuration task list, instructions for starting tasks in
  view hardware configuration 964
system details 823
system information task
  instructions for starting 852
system input/output configuration analyzer 859
system input/output configuration analyzer task 860
system management tasks
  energy management
    set power cap 806
    set power saving 809
system remote customization task list, instructions for starting tasks in
  account information 442
systems management tasks
  configuration
    transmit vital product data 869
    view frame layout 962
  monitor
    monitors dashboard 671
  service
    service status 804

T

task progress
  multiple objects 864
  single objects 865
task, user management 873
tasks
  configuration
    view frame layout 962
  load from removable media or server task 646
  monitor
    monitors dashboard 671
  object locking settings 688
  release I/O path 786
  service
    service status 804
  view licenses 967
TKE commands
  changing permission 429
TOD clock
  manually setting 482
toggle lock task 865
transmit service data task
  instructions for starting 866
transmit vital product data task 869
trusted key entry (TKE) feature
  logical partition cryptographic controls, required settings for
  customizing in activation profiles 505
two-way chat 419
TYPE keyword, input/output configuration 622

U

UDX
  configuring user defined extensions (UDX) 430
update HOM and VPD task 871
update I/O world wide port number 871
Usage Domain Zeroize 384
usage domain,zeroizing 429
USB flash memory drive
  alternative 15
user interface
  expand controls 277
  navigation pane collapse 277
user management, customizing 873
user settings task 415, 933
users and tasks task 936, 937

V

View Cage Details 404
view console event task 959
view console events task 960
view console tasks performed 962
view cryptographic details 427
View Frame Layout 963
view frame layout task 962
view hardware configuration task 965
view internal code changes summary 966
view licenses task 967
view only tasks
  operating system messages 691
view service history task
  instructions for starting 757, 975
viewing
  console events 960
viewing internal code changes 852
viewing the input/output configuration data 859
viewing, instructions for 602

W

web browser
  remote power off or restart 450
welcome 990
wizard profile image,using 508
writer report to tape, input/output configuration 619

Z

zeroizing crypto 428
zeroizing usage domain 429