



System z
Hardware Management Console
Operations Guide
Version 2.11.1

SC28-6905-01

Level 01a





System z

Hardware Management Console

Operations Guide

Version 2.11.1

SC28-6905-01

Note:

Before using this information and the product it supports, read the information in “Safety” on page xi, Appendix I, “Notices,” on page 251, and *IBM Systems Environmental Notices and User Guide*, Z125-5823.

This edition, SC28-6905-01, applies to the IBM Hardware Management Console Application, Version 2.11.1. This edition replaces SC28-6905-00.

There might be a newer version of this document in a **PDF** file available on **Resource Link**. Go to <http://www.ibm.com/servers/resourcelink> and click **Library** on the navigation bar. A newer version is indicated by a lowercase, alphabetic letter following the form number suffix (for example: 00a, 00b, 01a, 01b).

© Copyright IBM Corporation 2011.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures	vii
----------------	------------

Tables	ix
---------------	-----------

Safety	xi
---------------	-----------

Safety notices	xi
World trade safety information	xi
Laser safety information	xi
Laser compliance	xi

About this publication	xiii
-------------------------------	-------------

How to view this guide	xiv
Accessibility	xiv
How to send your comments	xiv
What's new in version 2.11.1	xv
Revisions	xv
New and changed features	xv

Chapter 1. Introduction	1
--------------------------------	----------

User Interface (UI) styles for the Hardware Management Console	2
Tree style user interface	3
Classic style user interface	3
Enabling users to change interface style	3
Changing the user interface style	4
LDAP support for user authentication	4
IPv6 support	4
Context sensitive help	5
Disruptive tasks	6
Locking an object	7
About activation profiles	8
USB flash memory drive	10

Chapter 2. Starting the Hardware Management Console	11
--	-----------

Turning on the Hardware Management Console	11
Logging on to the Hardware Management Console	12

Chapter 3. Using the tree style user interface	15
---	-----------

Task bar	16
Navigation pane	17
Navigation toolbar	17
Navigation pane collapse and expand controls	17
Welcome	17
Systems Management	18
Ensemble Management	30
HMC Management	30
Service Management	32
Tasks Index	34
Work pane	35
Work pane table	36
Work pane title and breadcrumb trail	39
Work pane table footer	39

Work pane table toolbar	39
Topology	41
Status bar	44
Exceptions	44
Hardware Messages	44
Operating System Messages	44
Status overview	45
Object locking for disruptive tasks	45

Chapter 4. Using the classic style user interface	47
--	-----------

Hardware Management Console workplace	47
Selecting objects	48
Opening an object	49
Performing a task on an object	52
Object locking for disruptive tasks	54
Monitoring your hardware	55
Views and work area	56
Groups	59
Exceptions	70
Active tasks	72
Console actions	73
Task list	76
Books	79
Help	80

Chapter 5. Hardware Management Console tasks	81
---	-----------

Analyze Console Internal Code	81
Archive Security Logs	81
Audit and Log Management	82
Authorize Internal Code Changes	82
Backup Critical Console Data	83
Block Automatic Licensed Internal Code Change Installation	83
Certificate Management	84
Change Console Internal Code	85
Change Password	85
Configure 3270 Emulators	86
Configure Data Replication	86
Console Default User Settings	87
Console Messenger	87
Sending a broadcast message	88
Initiating a two-way chat	88
Copy Console Logs to Media	89
Create Welcome Text	89
Customize API Settings	90
Customize Auto Answer Settings	90
Customize Automatic Logon	91
Customize Console Date/Time	91
Customize Console Services	93
Customize Customer Information	94
Customize Modem Settings	95
Customize Network Settings	95
Customize Outbound Connectivity	97

Customize Product Engineering Access	99	Integrated 3270 Console	144
Customize Remote Service	99	Integrated ASCII Console	145
Customize Scheduled Operations.	100	Load	146
Customize User Controls	102	Load from Removable Media or Server.	147
Domain Security	103	PSW Restart.	147
Enable Electronic Service Agent	103	Reset Clear	148
Enable FTP Access to Mass Storage Media.	104	Reset Normal	149
Fibre Channel Analyzer	105	Single Object Operations	149
Format Media	106	Start All	150
Hardware Management Console Settings	106	Stop All	150
Installation Complete Report	108	Service	152
Logoff or Disconnect	108	Archive Security Logs	152
Manage Enterprise Directory Server Definitions	109	Backup Critical Data	153
Manage Print Screen Files	109	Perform Problem Analysis	153
Manage Remote Connections	110	Perform Transfer Rate Test	154
Manage Remote Support Requests	111	Report a Problem	154
Manage SSH Keys	111	Restore Critical Data	155
Manage Users Wizard	111	Service Status	155
Manage Web Services API	112	Transmit Service Data	156
Monitor System Events	112	View PMV Records	156
Network Diagnostic Information	113	View Service History	157
Object Locking Settings	114	Change Management.	159
Offload Virtual RETAIN Data to Removable Media	114	Alternate Support Element	159
Password Profiles	115	Alternate Support Element Engineering Changes (ECs)	161
Perform a Console Repair Action	115	Change Internal Code	161
Reassign Hardware Management Console	116	Concurrent Upgrade Engineering Changes (ECs)	162
Rebuild Vital Product Data	116	Engineering Changes (ECs).	163
Remote Hardware Management Console	117	Product Engineering Directed Changes	164
Report a Problem	117	Retrieve Internal Code	164
Restore Legacy HMC Data	118	Save Legacy Upgrade Data	165
Save Upgrade Data	118	Single Step Internal Code Changes	166
Save/Restore Customizable Console Data	119	Special Code Load.	167
Shutdown or Restart	120	System Information	168
Single Step Console Internal Code	121	Remote Customization	169
Tip of the Day	121	Customer Information	169
Transmit Console Service Data	122	Remote Service.	169
Transmit Vital Product Data	122	Support Element Operations Guide	170
User Patterns	123	Operational Customization.	171
User Profiles	124	Automatic Activation.	171
User Settings	126	Change LPAR Controls	172
Tree style user interface	126	Change LPAR Group Controls.	173
Classic style user interface	127	Change LPAR I/O Priority Queuing.	173
User Templates.	128	Configure Channel Path On/Off	174
Users and Tasks	130	Customize/Delete Activation Profiles	174
View Console Events	130	Customize Scheduled Operations.	175
View Console Information	131	Customize Support Element Date/Time	177
View Console Service History	132	Enable I/O Priority Queuing	177
View Console Tasks Performed	132	Logical Processor Add	178
View Licenses	132	OSA Advanced Facilities	178
View PMV Records	133	Reassign Channel Path	179
View Security Logs	134	View Activation Profiles.	180
What's New	134	Object Definition	181
Chapter 6. Server tasks	137	Add Object Definition	181
Daily	138	Change Object Definition	182
Activate	138	Reboot Support Element.	182
Deactivate	139	Remove Object Definition	183
Grouping.	139	Configuration	184
Reset Normal	142	Edit Frame Layout	184
Recovery	144	Input/Output (I/O) Configuration Save and Restore	184
Access Removable Media	144		

System Input/Output Configuration Analyzer	185
System (Sysplex) Time	186
Transmit Vital Product Data	186
View Frame Layout	187
Energy Management	188
Set Power Cap	188
Set Power Saving	188
Monitor	190
Environmental Efficiency Statistics	190
Monitors Dashboard	190
Monitor System Events	192
z/VM Virtual Machine Management	194
Activate	194
Choose z/VM Virtual Machines to Manage	195
Deactivate	195
Edit the VMRM Active Configuration File	196
Grouping	196
Maintain z/VM Profiles	198
Maintain z/VM Prototypes	198
Maintain z/VM Virtual Machines to Manage	199
Maintain z/VM Volume Space	199
Undefine z/VM Virtual Machines for Management	200
View the VMRM Measurement Data	200
z/VM Virtual Network Information	201

Appendix A. Tasks and default user IDs 203

Appendix B. Enhanced driver maintenance 209

Switch points	209
Concurrent Upgrade Engineering Changes (EC) task	209
Preload	210
Activate	211
Query function availability from last activate	213
Completing the upgrade	213

Appendix C. Remote operations . . . 215

Using a remote Hardware Management Console	216
Using a web browser	217
Web browser requirements	218
Getting ready to use the web browser	219
Configuring the Hardware Management Console for web browser access from LAN or telephone connections	219
Logging on the Hardware Management Console from a LAN connected web browser	219

Configuring the Hardware Management Console for web browser access by telephone connections	220
---	-----

Appendix D. Remote support facility 223

Choose a connectivity method for remote support	223
Modem connectivity	223
Internet connectivity	224
Using multiple call-home servers	226

Appendix E. Using the System (Sysplex) Time task 229

Timing network	230
Network configuration	231
ETR configuration	232
ETR status	232
STP configuration	232
STP status	232
ETS configuration	233
PPS control	235
STP terminology	236

Appendix F. Changing your time-of-day clock 239

Setting the Hardware Management Console date and time	239
Setting the Support Element time zone	239
Setting the Support Element time	240
Time source enabled	240
Time source not enabled	240

Appendix G. Customizable data replication 243

Example 1: Peer-to-peer replication	244
Example 2: Master-to-slave replication	246
Data replication	248

Appendix H. Installing software from a mass storage device 249

Appendix I. Notices 251

Trademarks	252
Electronic emission notices	252

Index 257

Figures

1. Hardware Management Console configuration in a single CPC environment	1	33. Work area menu	49
2. Hardware Management Console configuration in a multiple CPC environment	2	34. Groups view	50
3. Context sensitive help not enabled	5	35. CPC pop-up menu	51
4. Context sensitive help enabled	6	36. CPC details window	51
5. Disruptive task confirmation window	7	37. Direct Manipulation.	53
6. View activation profile default window	8	38. Message window for invalid target objects	53
7. CPC details window	9	39. Unacceptable status	55
8. Change object options window	9	40. Exceptions work area	56
9. Select media device window	10	41. Workplace pop-up menu	57
10. Hardware Management Console initialization window	11	42. Classic groups work area	59
11. Hardware Management Console welcome window	12	43. CPC images group window	61
12. Hardware Management Console log on window	12	44. Defined CPCs group window	62
13. Tree style user interface Hardware Management Console workplace window	16	45. z/VM virtual machines work area	68
14. Task bar.	16	46. Virtual machine details window.	68
15. Systems Management Window	19	47. Exceptions work area	70
16. Systems management systems window	20	48. Console actions work area	73
17. Tasks pad	22	49. Task list work area	76
18. Vertical tasks pad	23	50. Create pattern match group window	141
19. Context menu.	24	51. Create pattern match group window for virtual machines	197
20. Tasks menu	25	52. Concurrent upgrade engineering changes (ECs) task window.	210
21. Systems management images window	26	53. Preload options	210
22. z/VM virtual machines	27	54. Activate option	212
23. Tasks using an alphabetical sort with icon style	31	55. Remote operation configuration	215
24. Tasks using a categorized sort with tile style	33	56. Asynchronous PCS connections via modems	220
25. Tasks index	35	57. Modem connectivity	224
26. Work pane table features	36	58. SSL connectivity	225
27. System management work pane table	37	59. SSL with proxy server connectivity	225
28. Custom table view	38	60. System (Sysplex) Time window	230
29. Systems views menu	41	61. STP status page.	233
30. Topology view features	42	62. ETS configuration page using the NTP option	234
31. Status overview	45	63. ETS configuration page using the NTP with PPS option	235
32. Classic style user interface Hardware Management Console workplace window	47	64. PPS control page	236
		65. Configure customizable data replication window - example 1	245
		66. Configure customizable data replication window - example 2	247

Tables

1.	Version codes and corresponding Support Element Operations Guide	xiii
2.	Hardware Management Console tasks and default user IDs.	203
3.	Tasks performed on objects and default user IDs	205
4.	Ports used by a remote Hardware Management Console for communications . .	216
5.	Ports used by a web browser for communications to the Hardware Management Console	217

Safety

Safety notices

Safety notices may be printed throughout this guide. **DANGER** notices warn you of conditions or procedures that can result in death or severe personal injury. **CAUTION** notices warn you of conditions or procedures that can cause personal injury that is neither lethal nor extremely hazardous. **Attention** notices warn you of conditions or procedures that can cause damage to machines, equipment, or programs.

World trade safety information

Several countries require the safety information contained in product publications to be presented in their translation. If this requirement applies to your country, a safety information booklet is included in the publications package shipped with the product. The booklet contains the translated safety information with references to the US English source. Before using a US English publication to install, operate, or service this IBM® product, you must first become familiar with the related safety information in the *Systems Safety Notices*, G229-9054. You should also refer to the booklet any time you do not clearly understand any safety information in the US English publications.

Laser safety information

All System z® models can use I/O cards such as PCI adapters, ESCON®, FICON®, Open Systems Adapter (OSA), InterSystem Coupling-3 (ISC-3), or other I/O features which are fiber optic based and utilize lasers or LEDs.

Laser compliance

All lasers are certified in the US to conform to the requirements of DHHS 21 CFR Subchapter J for Class 1 or Class 1M laser products. Outside the US, they are certified to be in compliance with IEC 60825 as a Class 1 or Class 1M laser product. Consult the label on each part for laser certification numbers and approval information.

CAUTION: Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. (C027)

CAUTION: This product contains a Class 1M laser. Do not view directly with optical instruments. (C028)

About this publication

This publication guides you while using the Hardware Management Console (HMC), assists you when navigating through the user interfaces, and describes the tasks you can use on the console and for selected systems. You can use it for the following IBM System z processors:

- IBM zEnterprise™ 196 (z196) and IBM zEnterprise z114 (z114).
- IBM System z10® Enterprise Class (z10™ EC) and IBM System z10 Business Class (z10 BC)
- IBM System z9® Enterprise Class (z9® EC) and IBM System z9 Business Class (z9 BC)
- IBM eServer™ zSeries® 990, 890, 900, and 800 (z990, z890, z900, and z800, respectively)

Use this publication along with the *Hardware Management Console Operations Guide for Ensembles*, SC27-2615, for information on the IBM zEnterprise Unified Resource Manager (zManager) tasks.

If you have a z196, z114, z10 EC, z10 BC, z9 EC, z9 BC, z990, or z890, your processor will operate only in logically partitioned (LPAR) mode. For all other processors previously listed, both LPAR and basic modes are available.

Notes:

- The task windows and user interface screens represented in this document are general samples. They may or may not represent the exact windows that are displayed for your user ID or version.
- The terms *system*, *server*, *object*, and *CPC* are used interchangeably through out this publication.

Not all code enhancements described in this guide may be available on your Support Element. Locate the version of code installed in your Support Element by looking at the title bar on the workplace window or click **SE Version** from the Welcome pane in the tree style user interface. Then refer to Table 1 to locate the *Support Element Operations Guide* that matches that version of the code installed in your Support Element. You can also find the version by using the **System Information** task under the Change Management task list.

Table 1. Version codes and corresponding Support Element Operations Guide

Version Code	Order Number
2.11.1	SC28-6906
2.11.0	SC28-6896
2.10.2	SC28-6882
2.10.1	SC28-6879
2.10.0	SC28-6868
2.9.2	SC28-6860
2.9.1	SC28-6858
2.9.0	SC28-6845
1.8.2	SC28-6831
1.8.0	SC28-6820
1.7.3	SC28-6818
1.7.2	SC28-6813
1.7.1	SC28-6811
1.7.0	SC28-6802
1.6.2	GC38-0615

Table 1. Version codes and corresponding Support Element Operations Guide (continued)

Version Code	Order Number
1.6.1	GC38-0607
1.6.0	GC38-0608
1.5.1	GC38-3119
1.5.0	GC38-3119

How to view this guide

If you are accessing the Hardware Management Console remotely, this guide is available in portable document format (PDF) to view or print from the Hardware Management Console as an online document or by accessing Resource Link® (<http://www.ibm.com/servers/resourcelink>).

When the PDF version of the guide opens, a list of bookmarks displays on the left side. These bookmarks display the highest level topics in the order that they appear as chapters in the book. If any of these topics have lower level topics, a + is displayed to the left of the higher level topic. To expand the topic, click once on the + and the next level will be displayed.

If you are accessing the Hardware Management Console locally, this guide is available in HTML format to view as an online document from the Hardware Management Console.

When the HTML version of the guide opens, you can scroll forward past the title page where the table of contents is displayed. You can click on any of the titles to view the information you are interested in. Use the **Forward** and **Back** buttons, located at the top of your window, to move around the document. Click **Close** when you are done viewing the document.

To get access to this guide in its online form while you are using the tree style user interface, see “Welcome” on page 17. If you are using the classic style user interface, see “Books” on page 79.

Accessibility

This publication is in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties using this PDF file you can request a web-based format of this publication. 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 request, 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.

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).

What's new in version 2.11.1

This guide reflects the licensed internal code for the Hardware Management Console Application, Version 2.11.1. You can tell if your Hardware Management Console has this version installed by looking at the title bar on the Hardware Management Console workplace window or by pointing your mouse over **HMC Version** in the top of the work pane window when using the tree style user interface. New enhancements to the version code are described in this guide.

There may 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.

Revisions

A technical change to the text is indicated by a vertical line to the left of the change.

New and changed features

This section summarizes the new and changed features for Version 2.11.1. You can also open the **What's New** task on the Hardware Management Console for a list of the enhancements.

This publication should be used in conjunction with the *Hardware Management Console Operations Guide for Ensembles Version 2.11.1*, SC27-2615. The *Hardware Management Console Operations Guide for Ensembles* focuses on the IBM zEnterprise Unified Resource Manager (zManager) tasks you can use on the Hardware Management Console. It also discusses the tasks that use the IBM zEnterprise BladeCenter® Extension (zBX) infrastructure.

The new and changed features for Version 2.11.1 include the following:

- The **WEB Services** tab has been added to the **Customize API Settings** task which enables and customizes the Web Services Application Programming Interface (API). The API can be used to query, configure, and control Central Processing Complexes (CPCs) containing a Support Element (SE). See the “Customize API Settings” on page 90 for more information on this new tab. You can also see the new publication, *System z Hardware Management Console Web Services API*, SC27-2616, on Resource Link for more information on the Web Services API.
- The **User Profiles** and **Manage Users Wizard** tasks adds the **Allow access to management interfaces** option. This option can enable or disable a particular Hardware Management Console (HMC) user profile permission to use the Application Programming Interfaces (APIs).
- The new **Manage Web Services API Logs** task is used to view or save the web services API logs. See “Manage Web Services API” on page 112 for more information.
- The **User Profiles** task adds an option that enables additional text input for a specified user ID before a task can be disrupted. If this option is enabled, the Disruptive Task Confirmation window requires additional text input from that user ID before the task is disrupted.
- Support was added to allow a secure FTP connection for transferring data on the Hardware Management Console and Support Element. The task changes include:
 - New **Manage SSH Keys** task allows you to import public keys associated with a host address. See “Manage SSH Keys” on page 111 for more information.
 - Updates to the **Change Console Internal Code** and **Retrieve Internal Code Changes** tasks. The option, **Use secure FTP**, was added enabling the secure transfer of data.
 - Updated **Customize Scheduled Operations** task, the **Audit and Log Management** operation. The **Offload using secure file transfer** option was added enabling the offloading of the audit data to a secure FTP connection.

- A new task, **View PMV Records**, was added to obtain Problem Management Viewable (PMV) records that were issued to the IBM Service Support System for the console or selected servers (CPCs). See the “View PMV Records” on page 133 console task or see the “View PMV Records” on page 156 server task for more information.
- The **CIM** tab has been added to the **Customize API Settings** task which enables the Common Information Model (CIM) interface. The CIM option has been removed from the **Customize Console Services** task.
- The API publications have been removed from the Hardware Management Console. A link from the tree style user interface is provided to Resource Link to access those publications.

Chapter 1. Introduction

The Hardware Management Console (HMC) communicates with each Central Processor Complex (CPC) through the CPC's Support Element (SE). When tasks are performed at the Hardware Management Console, the commands are sent to one or more Support Elements which then issue commands to their CPCs. CPCs can be grouped at the Hardware Management Console so that a single command can be passed along to as many as all of the CPCs defined to the Hardware Management Console. One Hardware Management Console can control up to 100 Support Elements and one Support Element can be controlled by 32 Hardware Management Consoles. Refer to Figure 1 and Figure 2 on page 2 for typical Hardware Management Console configurations.

This chapter briefly describes some of the concepts and functions of the Hardware Management Console, including the two user interfaces that are available when you use the Hardware Management Console.

The concepts and functions include:

- "User Interface (UI) styles for the Hardware Management Console" on page 2
- "LDAP support for user authentication" on page 4
- "IPv6 support" on page 4
- "Context sensitive help" on page 5
- "Disruptive tasks" on page 6
- "About activation profiles" on page 8
- "USB flash memory drive" on page 10.

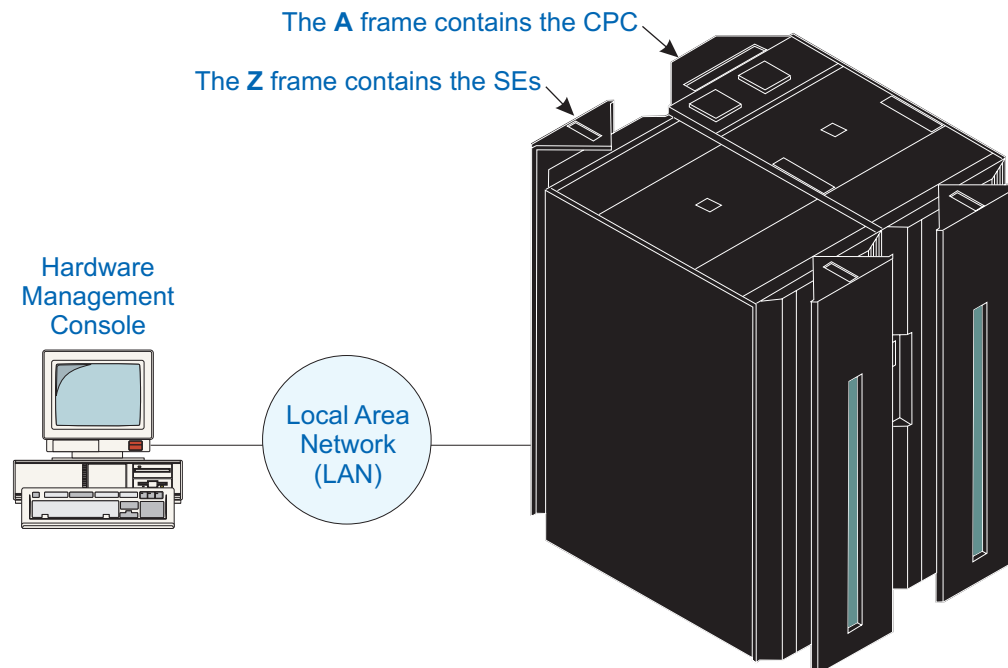


Figure 1. Hardware Management Console configuration in a single CPC environment

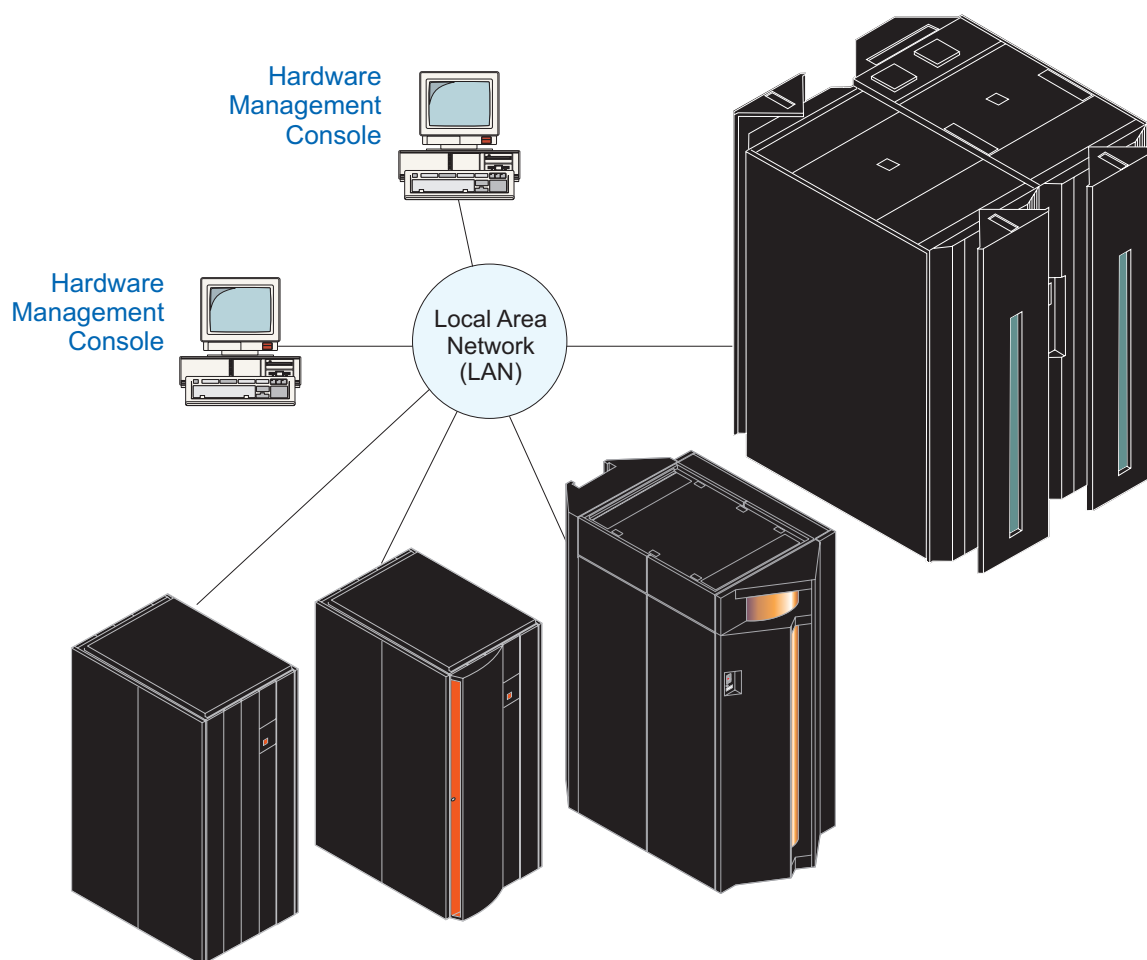


Figure 2. Hardware Management Console configuration in a multiple CPC environment

User Interface (UI) styles for the Hardware Management Console

The Hardware Management Console allows you to choose the interface style in which you prefer to work:

- Tree style user interface
- Classic style user interface (an older interface with object-oriented design).

For Hardware Management Consoles at Version 2.10.0 and later, the **tree style user interface** (tree interface) is the default user interface for Operator, Advanced Operator, Access Administrator, and System Programmer user roles. However, if you were using the classic style user interface prior to Version 2.10.0 you will continue to use the classic user style interface as your default interface unless you change it using the **User Settings** task. The Service Representative user role continues to use the classic style user interface as the default interface.

Also, if you changed the user interface style and you decide to upgrade to the next Hardware Management Console version the user interface style you were working with will not change.

Tree style user interface

The tree style navigation provides hierarchical views of system resources and tasks using drill-down and launch-in-context techniques to enable direct access to hardware resources and task management capabilities.

The tree style user interface also utilizes common terminology where possible. For example, instead of referring to *CPC*, a more general term of *server* is used for this interface. Similarly, in the tree interface *partitions* are equivalent to *images* in the classic interface.

See Chapter 3, “Using the tree style user interface,” on page 15 for more information on the tree style user interface for the Hardware Management Console.

Classic style user interface

The Hardware Management Console **classic style user interface** (classic interface) is the original user interface. The Service Representative user role uses this interface as its default interface. It has an object-oriented design. Through this design, you can directly manipulate the objects (such as CPCs or images) that are defined to the Hardware Management Console, and be aware of changes to hardware status as they are detected.

There are workplace layout choices you can use when you are working with the console actions. You control these choices from the **User Settings** task or by selecting the **Style Settings** option on the context menu. The original, classic interface layout is the default for the Console Actions Work Area. The additional layout settings allow you to display the console actions as a list or display them in predefined groups. These console actions can be presented in the original, classic order or ascending alphabetical order by task name. You can also hide areas of the workplace allowing you to display more tasks in the work area you are currently working.

You can work with the objects on the workplace using the mouse to select them. There are several techniques for manipulating objects and tasks. One way to do this is to left-click an object to select it and double-click the task. (Refer to “Performing a task on an object” on page 52.) An alternate method is known as the *drag and drop technique*, which involves using the mouse to pick up one or more objects, dragging them to a task, and then dropping them. These techniques are examples of what is known as *direct manipulation*.

See Chapter 4, “Using the classic style user interface,” on page 47 for more information on using the classic style user interface for the Hardware Management Console.

Enabling users to change interface style

If the **UI Style** tab is not displayed when you open the **User Settings** task, then you are not allowed to change the interface style on the Hardware Management Console. Your access administrator has the ability to enable users to change interface styles and to change the default interface style for the Hardware Management Console by performing the following steps:

1. Log on the Hardware Management Console using the ACSADMIN default user ID or a user ID that has the predefined Access Administrator roles.
2. Open the **Console Default User Settings** task:
 - Using the tree interface: Open the **Console Default User Settings** task from the **HMC Management** or **Tasks Index** work panes.
 - Using the classic interface: Open **Console Actions** under **Views**, then open the **Console Default User Settings** task.
3. The Console Default User Settings window is displayed.
4. Click the **UI Style** tab.

- To enable users to change the user interface style, select **Allow user to change the UI style**, then click **Apply**.
 - To control the default user interface style for the Hardware Management Console, select **Tree Style** or **Classic Style**, then click **Apply**.
5. Click **OK** when you have completed this task.

Changing the user interface style

If the Hardware Management Console is configured to enable you to change the user interface style, you can change interface styles by using the **User Settings** task.

To change from the tree interface back to the classic interface, perform the following steps:

1. Open the **User Settings** task (from the **HMC Management** or **Tasks Index** work panes or click on the user ID from the task bar). The User Settings window is displayed.
2. Click the **UI Style** tab. The User Style Information window is displayed.
3. Select **Classic Style**, then click **Apply**. The interface style changes to classic and the **User Settings** task can be located under the **Active Tasks** icon.

To change from the classic interface back to the tree interface, perform the following steps:

1. Open the **User Settings** task (under **Console Actions**). The **User Settings** window is displayed.
2. Click the **UI Style** tab. The User Style Information window is displayed.
3. Select **Tree Style**, then click **Apply**.
4. Click **OK**.

LDAP support for user authentication

Lightweight Directory Access Protocol (LDAP) support for Hardware Management Console user authentication allows a Hardware Management Console to be configured to use an LDAP server to perform user ID and password authentication at logon time. The user ID is defined on the Hardware Management Console along with the roles to be given to the user ID (see “User Profiles” on page 124). Hardware Management Console settings related to the user ID will continue to reside on the Hardware Management Console, and the LDAP directory will be used to authenticate the user, therefore eliminating the need to store the user ID's password locally. Both SSL and non-SSL connections to the LDAP server are supported.

This function is designed to more easily assist system administrators in the creation of Hardware Management Console user IDs matching existing company user names and to eliminate the need to create and distribute passwords when this is already being managed by an LDAP accessible corporate control mechanism. This can also help meet corporate security guidelines.

IPv6 support

The Hardware Management Console, Version 2.10.0 and later, supports the IPv6 protocol. It can communicate using IPv4 (TCP/IP Version 4), IPv6 (TCP/IP Version 6), or both. The IPv6 protocol was developed by the Internet Engineering Task Force to address the limitations in the existing IPv4 protocol, particularly, the limited number of IPv4 addresses. For more detailed information on IPv6, see <http://www.ipv6.org>.

Whenever you need to specify a TCP/IP address, you have the option of specifying an IPv4 or IPv6 TCP/IP address.

The IPv4 address is written as four decimal numbers, representing four bytes of the IP address, separated by periods (for example, 9.60.12.123).

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).

In most cases, you will specify a domain name to avoid having to remember and specify the complicated IPv6 addresses.

Note: The domain name is translated to an IP address if a DNS server has been defined. Use the **Customize Network Settings** task to enable DNS.

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). Every time a new task window opens you need to click **i** to enable context sensitive help.

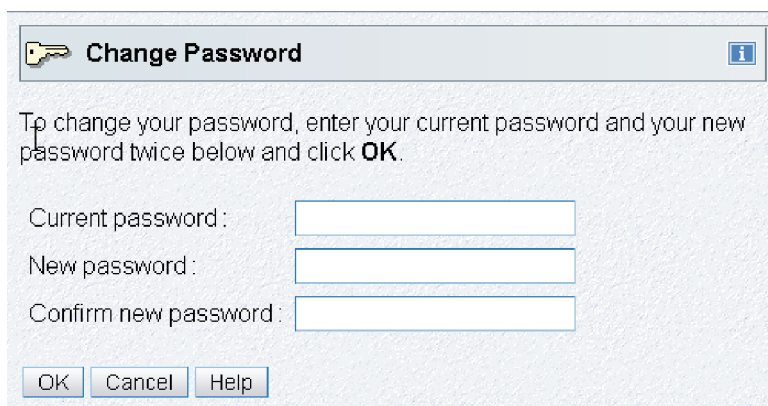


Figure 3. Context sensitive help not enabled

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 6). 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.

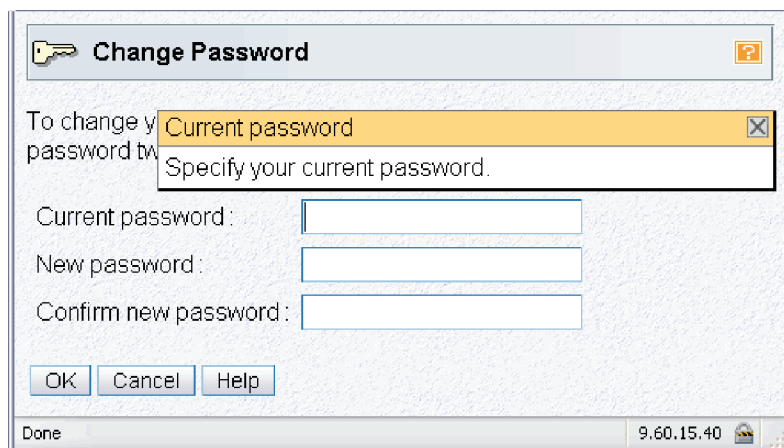


Figure 4. Context sensitive help enabled

- 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 Hardware Management Console tasks can be considered *disruptive*. 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
- **Object Definition Tasks:** Reboot Support Element
- **Configuration Tasks:** System (Sysplex) Time

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 7 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.

 **Disruptive Task Confirmation : Deactivate - GDLVMBUV**
i

Attention: The Deactivate task is disruptive.

Executing the Deactivate task may adversely affect the objects listed below. Review the confirmation text for each object before continuing with the Deactivate task.

Objects that will be affected by the Deactivate task

System Name	Type	OS Name	Status	Confirmation Text
GDLVMBUV:CECSIMVM	Image	GDLVMBUV	Operating	Deactivate causes operations to be disrupted, since the target is currently in use and operating normally.
GDLVMBUV:ZLNX	Image		Operating	Deactivate causes operations to be disrupted, since the target is currently in use and operating normally.
GDLVMBUV:ZVM53	Image	ZVMV5R30	Operating	Deactivate causes operations to be disrupted, since the target is currently in use and operating normally.
GDLVMBUV:ZVM54	Image	ZVMV5R40	Operating	Deactivate causes operations to be disrupted, since the target is currently in use and operating normally.
GDLVMBUV:ZVM61	Image	ZFWVMTS1	Operating	Deactivate causes operations to be disrupted, since the target is currently in use and operating normally.

Do you want to execute the Deactivate task?

Type the password below for user "SYSPROG" then click "Yes".

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. You can use the online 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 Profiles** 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.

Locking an object

You may want to lock an object preventing you from accidentally performing a disruptive task on the object. Unlock the object only when you want to perform a disruptive task on the object.

Note: The **Lockout disruptive task** setting only affects operations from the Hardware Management Console workplace that you are currently working at and its web browser. It does not affect any operations at the Support Element or operations initiated from other Hardware Management Consoles.

For more information on locking an object see “Object locking for disruptive tasks” on page 45 when using the tree interface or see “Object locking for disruptive tasks” on page 54 when using the classic interface.

About activation profiles

Activation Profiles are required for CPC and CPC image activation. They are used to tailor the operation of a CPC and are stored in the Support Element associated with the CPC. There are four types of activation profiles:

Reset: Every CPC in the processor cluster needs a reset profile to determine the mode in which the CPC licensed internal code will be loaded and how much central storage and expanded storage will be used. The maximum number of reset profiles allowed for each CPC is 26.

Image:

If logically partitioned (LPAR) mode has been selected in the reset profile, each partition has an image profile. The image profile determines the number of CPs that the image will use and whether these CPs will be dedicated to the partition or shared. It also allows you to assign the amounts of central storage and expanded storage to be used by each partition. Depending on the Support Element model and machine type, the maximum number of image profiles allowed for each CPC can be between 64 and 255.

Load: A load profile is needed to define the channel address of the device from which the operating system will be loaded. Depending on the Support Element model and machine type, the maximum number of load profiles allowed for each CPC can be between 64 and 255.

Group:

A group profile defines the group capacity value that can be customized in determining the allocation and management of processor resources assigned to the logical partition in a group. This profile will not contain the name(s) of the LPAR images that make up the group.

Default profiles of each of these types are provided. The default profiles can be viewed (see Figure 6), copied to create new profiles, and modified using the **Customize/Delete Activation Profiles** task. (Refer to “Operational Customization” on page 171 for more information.)

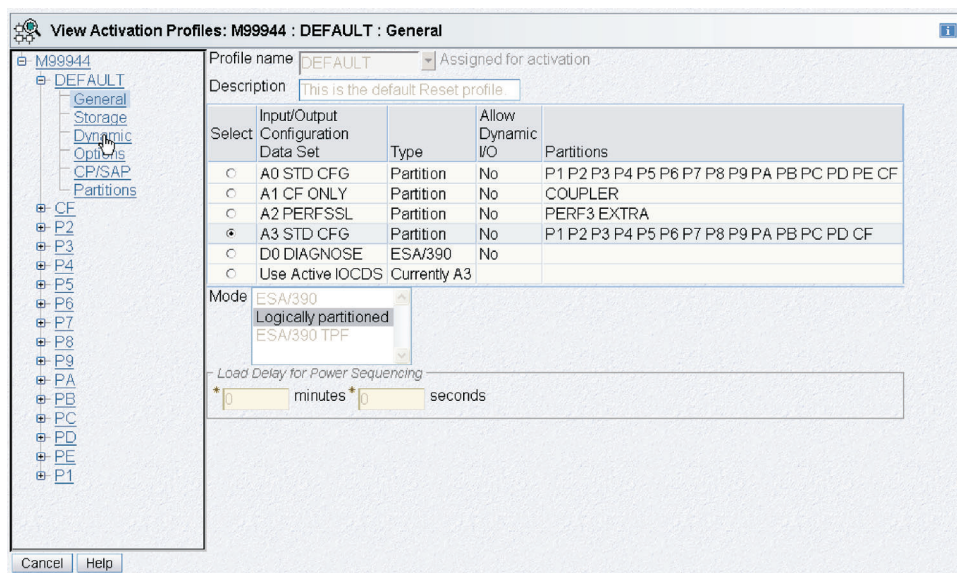


Figure 6. View activation profile default window

The **Activate** task activates the CPC or CPC image. Initially, the Default profile is selected. You may specify an activation profile other than the Default by selecting the desired CPC or CPC image icon in the list.

Another method to specify a different activation profile is by using the **Change Options...** window as shown in Figure 7. You can click this to display a window allowing you to select a different profile name as shown in Figure 8. (Refer to “Displaying CPC or image details” on page 50 for more information.)

Figure 7. CPC details window

The activation profile corresponding to the CPC or image of the Details window is effective when the **Activate** task is performed on the object.

Select	Profile Name	Type	Profile Description
☐	5ZONES	Reset	This is the default Reset profile.
☒	DEFAULT	Reset	This is the default Reset profile.
☐	JA2	Reset	This loads Ptero with valid definitions
☐	MORELPARS	Reset	This loads Ptero with valid definitions
☐	SIMPLE1	Reset	Profile for SCLP testing
☐	T03START	Reset	This loads Ptero with valid definitions
☐	ANEWLOADPROFILE0	Load	This is a brand new load profile for use to exerci
☐	DEFAULTLOAD	Load	This is the default Load profile.
☐	I5553TEST	Load	test load profile for I5553
☐	LINUXLOAD	Load	Use this to run Linux. Only run one at a time!
☐	ZVM	Load	Use this to run z/VM. Only run one at a time!

Figure 8. Change object options window

For more detailed information on activation profiles, see the *Support Element Operations Guide*.

USB flash memory drive

The Hardware Management Console Version 2.11.0 introduces a new removable writeable media as an alternative to the Hardware Management Console DVD-RAM. The tasks that require access to a DVD-RAM now have the ability to access a USB flash memory drive. There can be more than one USB flash memory drive inserted into the console.

Note: If you are running a task that accesses a USB flash memory drive, you must be aware that there could be more than one USB flash memory drive in the console. Make sure you are accessing the correct USB flash memory drive for your task.

Also, running backup from the Hardware Management Console requires a USB flash memory drive inserted in the console. It is recommended that you install the USB flash memory drive in the Hardware Management Console and do not remove it. This is essential when you are running a backup scheduled operation.

Some of the tasks that require media allow you to choose the type of media depending on the system you are using. You can choose the type of media you want to send the data to from the Select Media Device window, as shown in Figure 9,

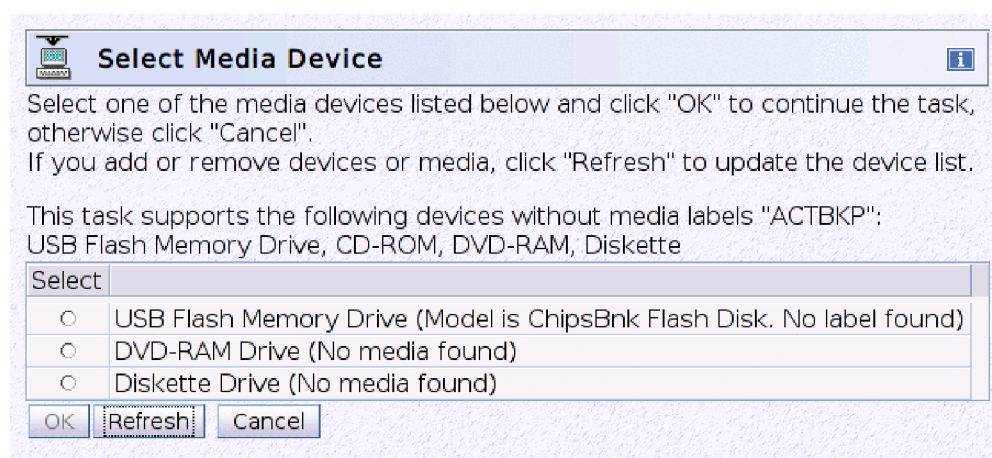


Figure 9. Select media device window

The Hardware Management Console Version 2.10.0 and later is no longer provided with a diskette drive. The available media is DVD-RAM, CD-ROM, and USB flash memory drive (formerly referred to as the memory key).

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 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.
- Tested virtual file allocation table (VFAT) USB flash memory drives include IBM 128MB, Lenovo 512MB and 1GB, and IBM packaged SMART™ drives.

Chapter 2. Starting the Hardware Management Console

This chapter assists you in starting the Hardware Management Console.

Turning on the Hardware Management Console

First, turn on the Hardware Management Console by setting both the display and system units to the *On* position. You should then see the Initialization window containing the IBM Logo and copyright information as shown in Figure 10.



Figure 10. Hardware Management Console initialization window

When initialization is complete, the Welcome window is displayed.

The Welcome window includes links for logging on to the Hardware Management Console and to the online help. It also includes status indicators and message icons. The status indicator reflects the current overall status of the defined CPCs 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 11 on page 12 for an example of the Welcome window.

All the windows of the Hardware Management Console also include a *title bar* that is displayed at the top of the window. The *title bar* identifies the name and the version of the Hardware Management Console you are currently working from. You can also minimize or maximize the Hardware Management Console or close the application from the title bar by clicking the appropriate icons in the upper right corner. The title bar may not always appear in the diagrams in this publication but it will always be

displayed on your console.



Figure 11. Hardware Management Console welcome window

Logging on to the Hardware Management Console

To log on to the Hardware Management Console, click **Log on and launch the Hardware Management Console web application.** from the Welcome window.

The Logon window is displayed as shown in Figure 12.

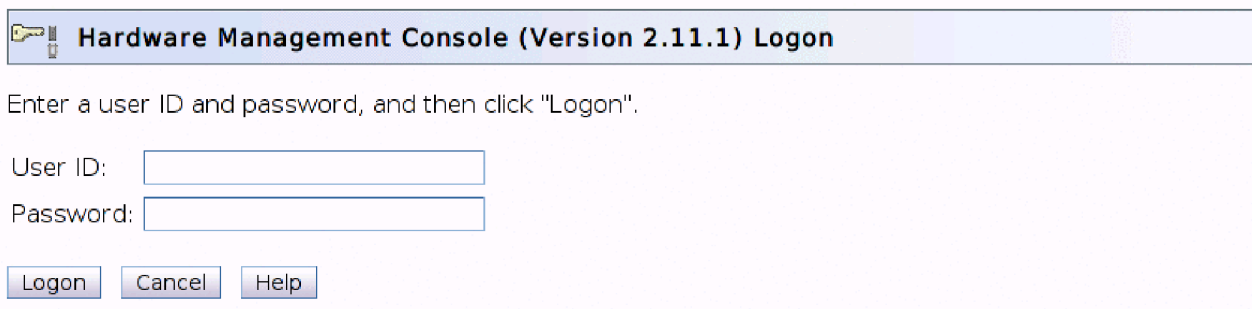


Figure 12. Hardware Management Console log on window

Default user IDs and passwords are established as part of a base Hardware Management Console. The Access Administrator **should assign new user IDs and passwords for each user and remove the default user IDs as soon as the Hardware Management Console is installed** by using the **User Profiles** task or the **Manage Users Wizard**. The predefined default user roles, user IDs, and passwords are:

Operator	OPERATOR	PASSWORD
Advanced Operator	ADVANCED	PASSWORD
System Programmer	SYSPROG	PASSWORD
Access Administrator	ACSADMIN	PASSWORD
Service Representative	SERVICE	SERVMODE
Ensemble Administrator	ENSADMIN	PASSWORD
Ensemble Operator	ENSOPERATOR	PASSWORD

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

To log on, enter one of the default user ID and password combinations, the user ID and password combination assigned to you by your Access Administrator, or your LDAP user ID (see “LDAP support for user authentication” on page 4). Then click **Logon**.

Note: If you are accessing the Hardware Management Console remotely and depending on the browser you are using, the entry fields and the **Logon** button may initially be hidden until the Logon window has completely loaded. Use the online help if you need additional information by clicking **Help** from the Logon window.

After you log on, the Hardware Management Console workplace window is displayed (see Figure 13 on page 16 and Figure 32 on page 47). If enabled, the Tip of the Day window is displayed (for more information see “Tip of the Day” on page 121).

The Hardware Management Console workplace window allows you to work with tasks for your console and CPCs (servers). Not all tasks are available for each user ID. See Appendix A, “Tasks and default user IDs,” on page 203 for a listing of all tasks and the default user IDs associated with the tasks.

If at any time you do not know or remember what user ID is currently logged on to the Hardware Management Console, click on the user ID located on the task bar in the tree style user interface, or open the **Users and Tasks** task in the classic style user interface.

Chapter 3. Using the tree style user interface

This chapter explains how to use the tree style user interface to perform tasks on the Hardware Management Console (HMC) or on your system resources. The tree style user interface is comprised of several major components as shown in Figure 13 on page 16:

- Banner
- Task bar
- Navigation pane
- Work pane
- Status bar.

The *banner*, across the top of the workplace window, identifies the product and logo. Use the **User Settings** task to turn off the banner.

The *task bar*, located below the banner, displays the name of any tasks that are running, the user ID you are logged in as, online help information, and a link to logoff or disconnect from the console.

The *navigation pane*, in the left portion of the window, contains the primary navigation links for managing your system resources and the Hardware Management Console. These 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. For example, when **Welcome** is selected in the navigation pane, the Welcome window content is displayed in the work pane, as shown in Figure 13 on page 16.

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.

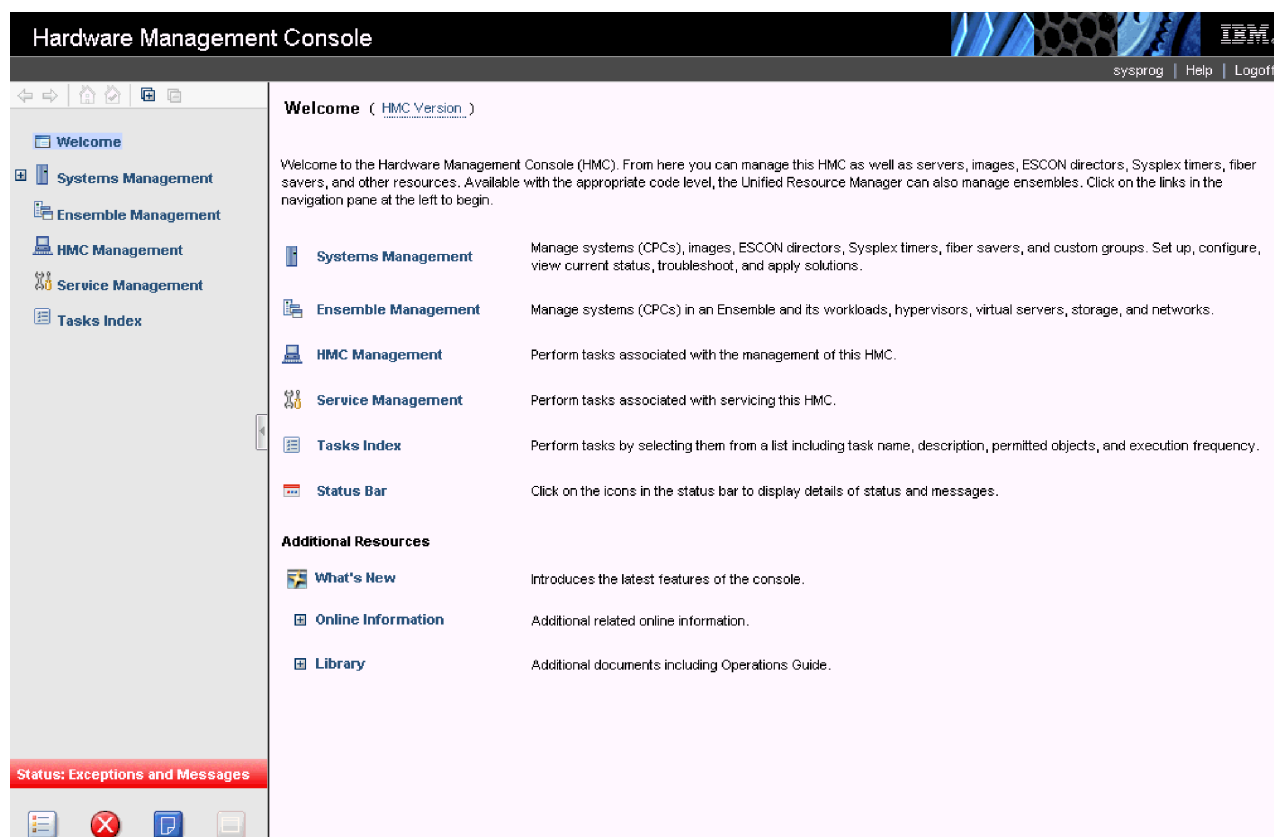


Figure 13. Tree style user interface Hardware Management Console workplace window

You can resize the panes of the Hardware Management 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 Systems Management work pane border that separates the resources table from the tasks pad.

Task bar

The task bar, located below the banner, acts as a navigation bar displaying tasks that have been opened and have not yet been closed. The task bar may be used as a navigation aid or as an 'active task switcher' to move between these tasks. The task switcher does not pause or resume existing tasks. Clicking on a task in the task bar brings that task's window forward and gives it focus. The right end of the task bar also contains the following information as shown in Figure 14.

- **user ID** that you are logged in as. By clicking the user ID you open the **User Settings** task.
- **Help** initially displays information on how to use the tree style user interface on the Hardware Management Console. It also provides information on all the Hardware Management Console tasks.
- **Logoff** opens the **Logoff or Disconnect** task.



Figure 14. Task bar

Navigation pane

The navigation pane, as shown in Figure 13 on page 16, contains the primary navigation links for managing your system resources and the Hardware Management Console. These include:

- Welcome
- Systems Management
- Ensemble Management (See the *Hardware Management Console Operations Guide for Ensembles* for more detailed information.)
- HMC Management
- Service Management
- Tasks Index

It also includes the following navigation methods you can use when working in the tree style workplace:

- Navigation toolbar
- Navigation pane collapse and expand controls

Navigation toolbar



The navigation toolbar, located above the navigation pane, consists of:

- Forward and backward buttons that allow you to move forward and backward in the selection history for the work pane.
- Home page and set home page buttons that allow you to return to the home page during your session and establish a home page to return to every time you log on to the Hardware Management Console.
- Expand and collapse buttons that allow you to expand and collapse all of the nodes of the navigation pane.

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 located on the border between the navigation pane and the work pane. You can click on these controls to collapse or expand the navigation pane allowing you more work area in the work pane, if required. Hovering over these controls indicates whether you are hiding or displaying the navigation pane. You can see an example of these controls in Figure 16 on page 20.

Welcome

Welcome work pane displays navigation information, the Hardware Management Console version information, and other helpful documentation (see Figure 13 on page 16).

To see the level of the Hardware Management Console you are currently working with and other pertinent information, point your mouse over **HMC Version** found at the top of the work pane.

The **Additional Resources** include:

- **What's New** introduces the latest features of this console. It is a wizard that provides high level information describing the new features in this version of the Hardware Management Console. It can also be found in the **Tasks Index** and **HMC Management** nodes of the navigation pane.

- **Online Information** provides a listing of the following online resources. Click on each item to access them.

Note: This information is available only when you are accessing the Hardware Management Console remotely.

- **Resource Link** - a web-based solutions site for more information on planning, installing, and maintaining System z servers and software.
- **Tutorials** - for additional information on using the Hardware Management Console tree style user interface and tasks.
- **APIs** - for access to the System z Application Programming Interface publications:
 - *Application Programming Interfaces* - provides information for developing system management applications that will provide integrated hardware and software system management solutions using the application programming interfaces.
 - *Application Programming Interfaces for Java* - describes the **com.ibm.hwmca.api** package. It provides information for developing system management applications that will provide integrated hardware and software system management solutions using the application programming interfaces. The purpose of this package is to allow remote Java applications the ability to exchange data related to the objects that the Console application manages.
 - *Common Information Model (CIM) Management Interface* - provides system programmers with instructions on how to manage their systems using Common Information Model (CIM) management interfaces on the Hardware Management Console.
 - *Hardware Management Console Web Services API* - defines, for reference purposes, the external interface of the Hardware Management Console (HMC) Web Services Application Programming Interface (Web Services API) for zEnterprise System, Version 2.11.1. This publication specifies the capabilities, input and output formats, and behaviors of the Web Services API as viewed by an application external to the HMC that is leveraging that interface.
- **Library** - lists the following online publications provided with the Hardware Management Console application. Click on each publication to access them.

Note: If you are accessing the Hardware Management Console remotely, PDF versions of the documents are available. If you are accessing the Hardware Management Console locally, HTML versions of the documents are available.

- *Coupling Facility Control Code Commands* - provides information about commands you can issue from the Support Element to coupling facility control code. It is available only online.
- *Coupling Facility Control Code Messages* - provides information about messages sent from coupling facility control code to the Support Element and Hardware Management Console. It is available only online.
- *Hardware Management Console Operations Guide* - provides information about managing your system using the Hardware Management Console. It is the book you are currently using.
- *Hardware Management Console Operations Guide for Ensembles* - provides information on the ensemble tasks used by the Hardware Management Console. This publication is used in conjunction with the *Hardware Management Console Operations Guide*.

To open an online book, locate the book you want to open and click on the book title. The book remains open until you close it. When you have finished viewing the book, close it by clicking the **X** in the upper right corner of the book window.

Systems Management



Systems 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 (see Figure 15):

- Systems
- Directors/Timers
- Fiber Savers
- Custom Groups
- Unmanaged Resources

Note: The **Unmanaged Resources** node is available only if your user ID is based on the access administrator or service representative task roles.

When you select **Systems Management** from the navigation pane, the following resource tabs can be displayed in the work pane (see Figure 15):

- All Resources
- Images
- z/VM[®] Virtual Machines
- Topology

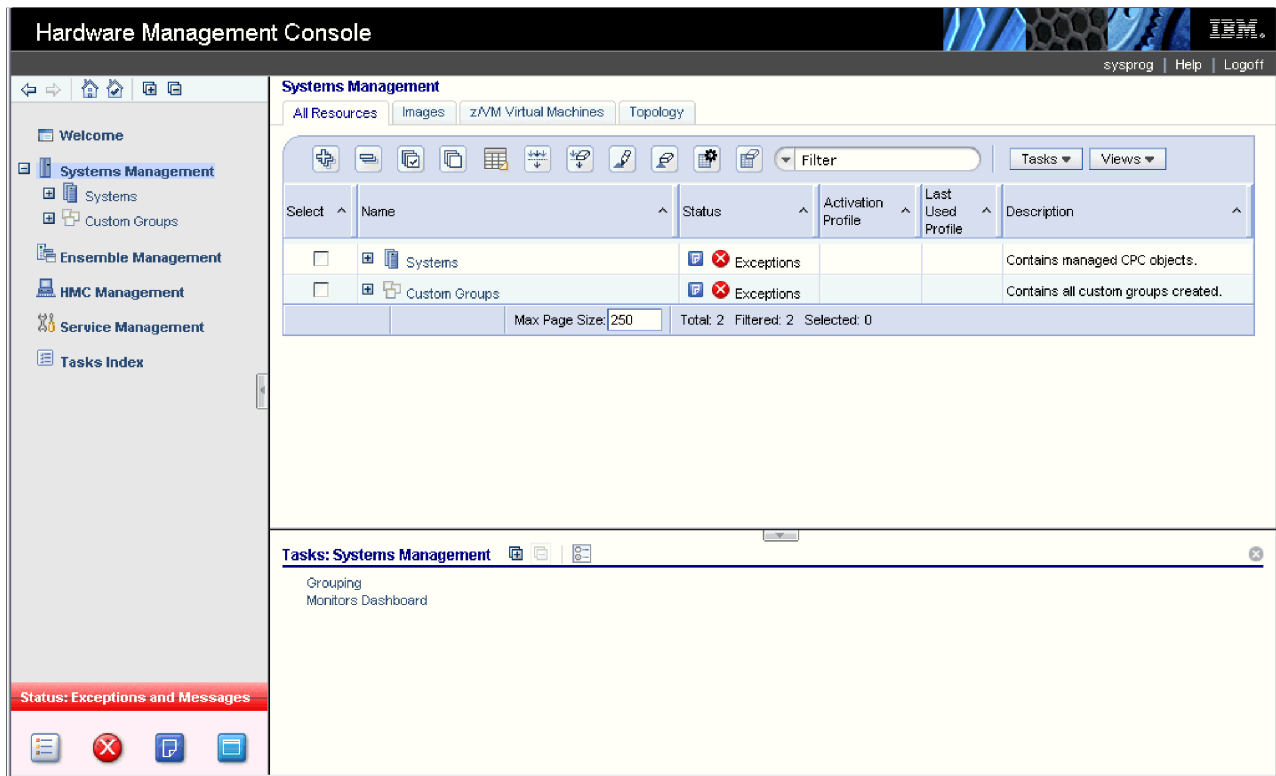


Figure 15. Systems Management Window

Systems

The **Systems** node represents all the resources that are managed by this Hardware Management Console.

When you select the **Systems** node from the navigation pane a listing of individually defined servers is displayed under the **Systems** node in the navigation pane. Also, the following resource tabs are displayed in the work pane (see Figure 16 on page 20):

Systems

Displays, in a table format, all managed systems.

Images

Displays, in a table format, a list of all LPAR images defined across all systems. An additional **System** column in the work pane table identifies the system to which each image is defined.

Note: The images are available from the **Systems** tab in a hierarchical format where you can sort or filter to get a similar view as from the **Images** tab.

For more information on system images, see “System images” on page 26.

z/VM Virtual Machines

Displays, in a table format, all managed z/VM Virtual Machines on all z/VM LPARs defined across all systems. If there are no z/VM Virtual Machines the tab is not displayed. For more information on z/VM virtual machines, see “z/VM virtual machines” on page 26.

Topology

Displays the objects using a graphical relationship based model instead of the default table format. See “Topology” on page 41 for more information.

To work with a system, you can perform one of the following actions:

- Select a system under the **Systems** node from the navigation pane
- Select a system name from the work pane table
- Click in the **Select** column next to the system name in the work pane table

Note: Working with one system at a time is the default and is used in the examples throughout this chapter. However, if you want to work with more than one system 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 systems to manage.

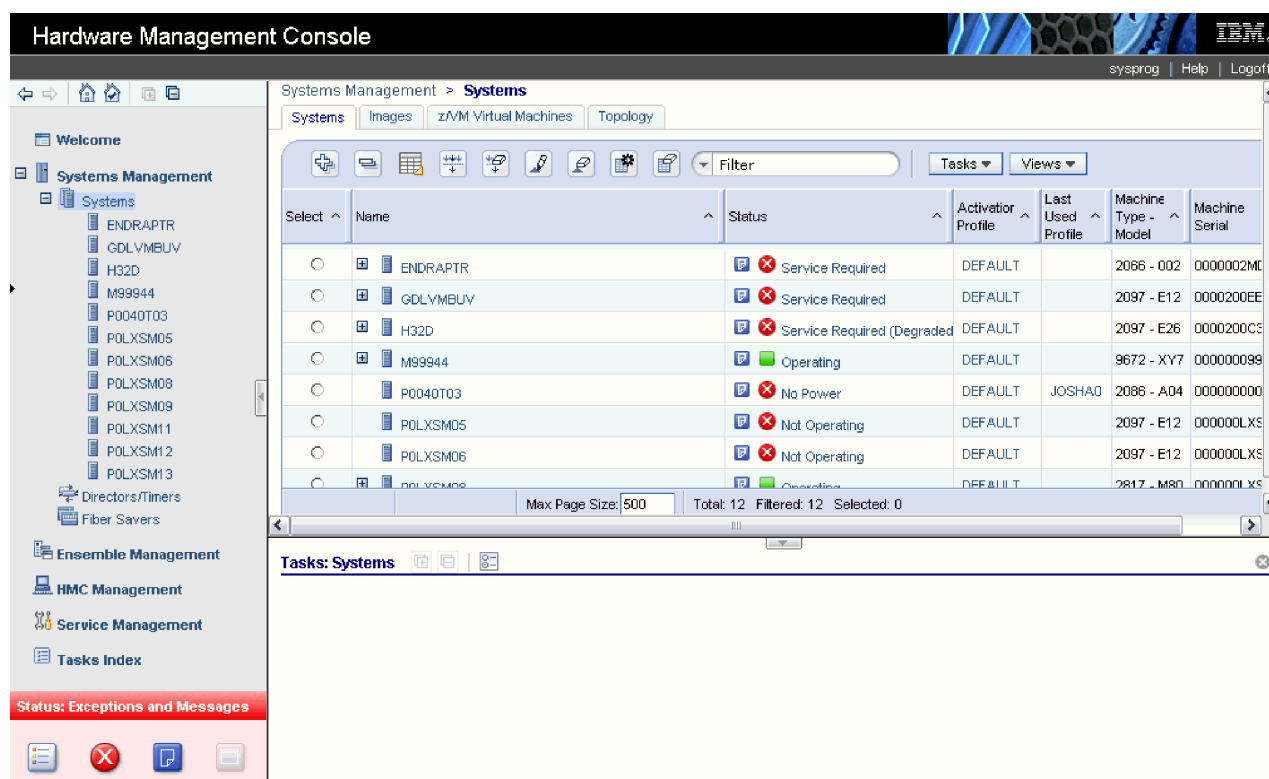


Figure 16. Systems management systems window

Tasks cannot be performed on a system until it is defined. The undefined systems are listed under the **Unmanaged Resources** node (see “Unmanaged Resources” on page 28). To define a system, see “Add Object Definition” on page 181.

Opening tasks for the system: Once you have chosen the systems (servers) 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 for tasks and are not tasks themselves.

- Daily
- Recovery
- Service
- Change Management
- Remote Customization
- Operational Customization
- Object Definition
- Configuration
- Energy Management
- Monitor
- z/VM Virtual Machine Management (displays if a server image is running z/VM V5.3 or later)

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 is displayed next to the server name (see “Context menu” on page 23)
- Click the **Tasks** menu from the work pane table toolbar (see “Tasks menu” on page 24)
- 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 a server the task is not displayed.

Tasks pad: The tasks pad is displayed below the work pane table after you have selected the managed objects with which you want to work with.

Figure 17 on page 22 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:

- **Tasks Index** or **HMC 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.

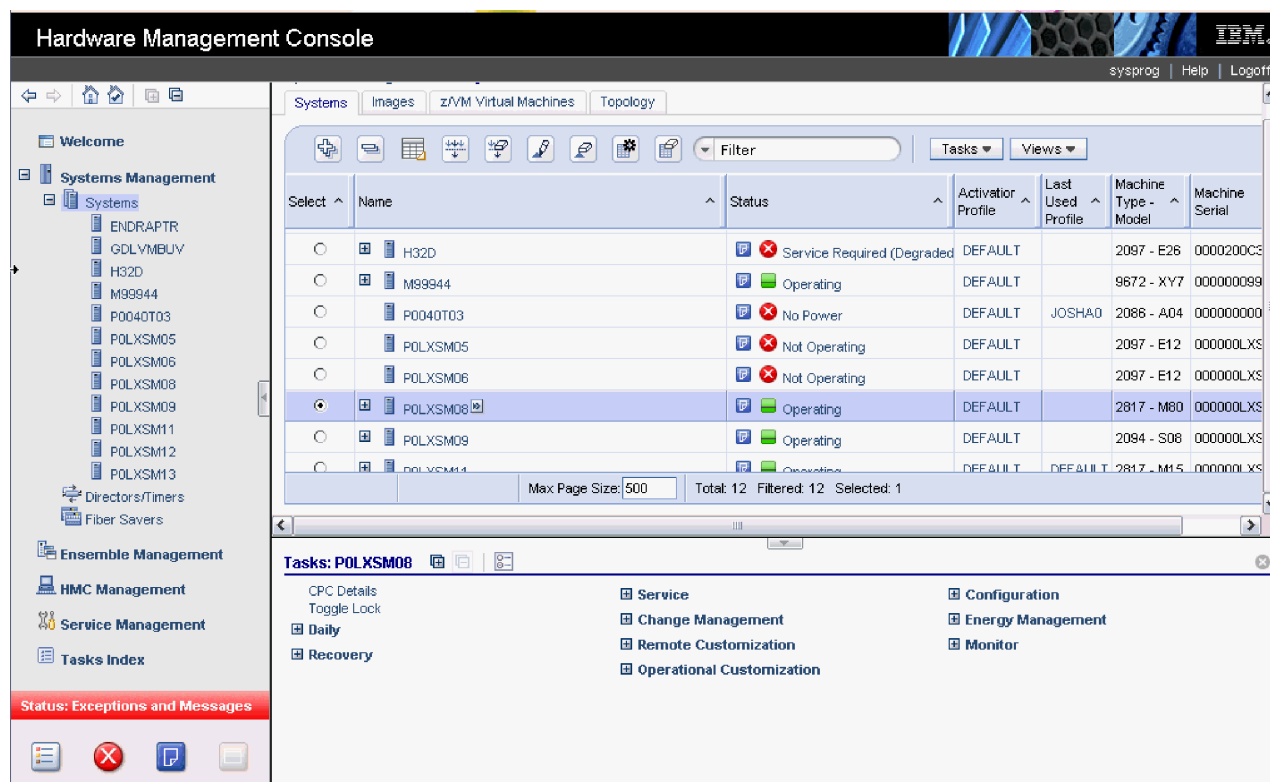


Figure 17. Tasks pad

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 Figure 18 on page 23 for an example).

Note: When the tasks pad displays vertically the column count is not available.

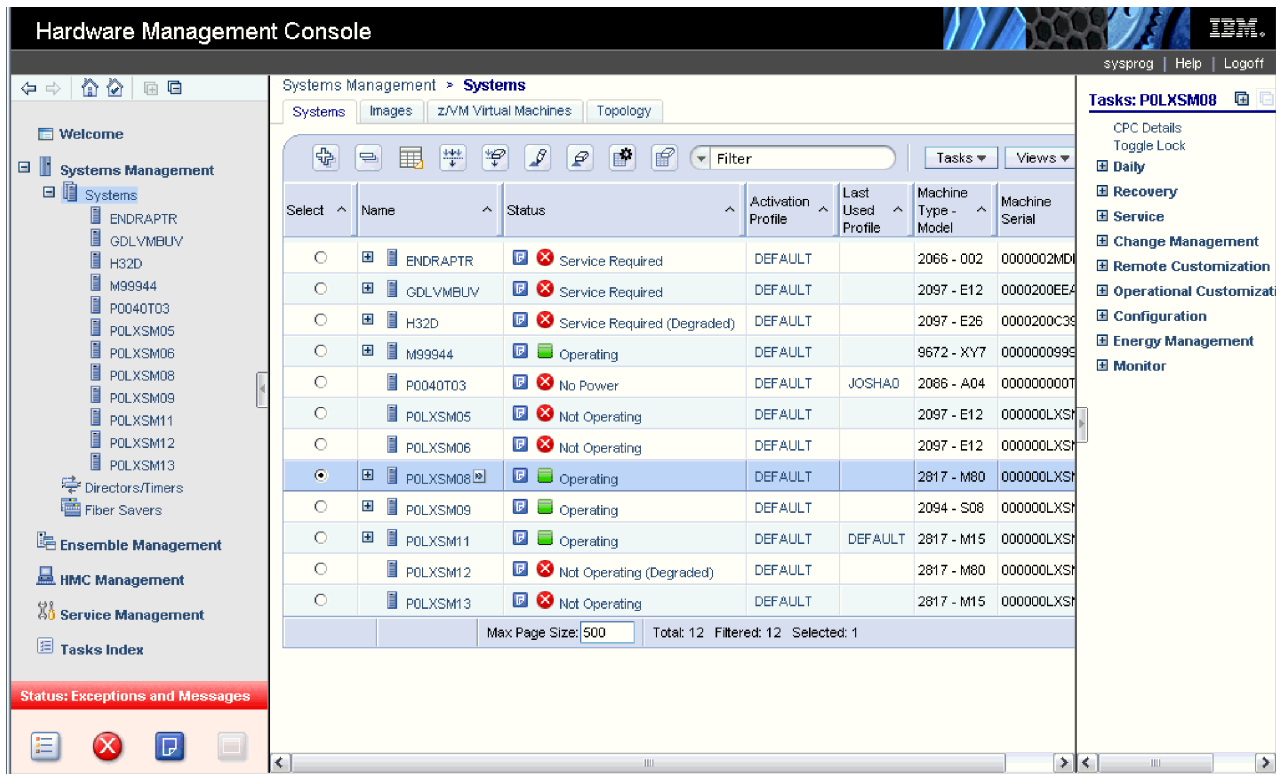


Figure 18. Vertical tasks pad

Figure 18 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 are shown in the tasks pad are those available to the user currently logged in.

An example of using the tasks pad method:

1. Select a server in the work pane table (click the **Select** column).
2. 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.

3. From the task group, select the task that you want to perform.
4. The task window is displayed.

Context menu: The context menu is a pop-up menu that lists the task groups associated with the selected object or objects. Context menus are available only for table selections. For example, in the **Select** column of the Systems work pane table, select the object or objects you want to work with. 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, as shown in Figure 19 on page 24. You can also right click within the table cell of the object name to display the context menu. Then 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.

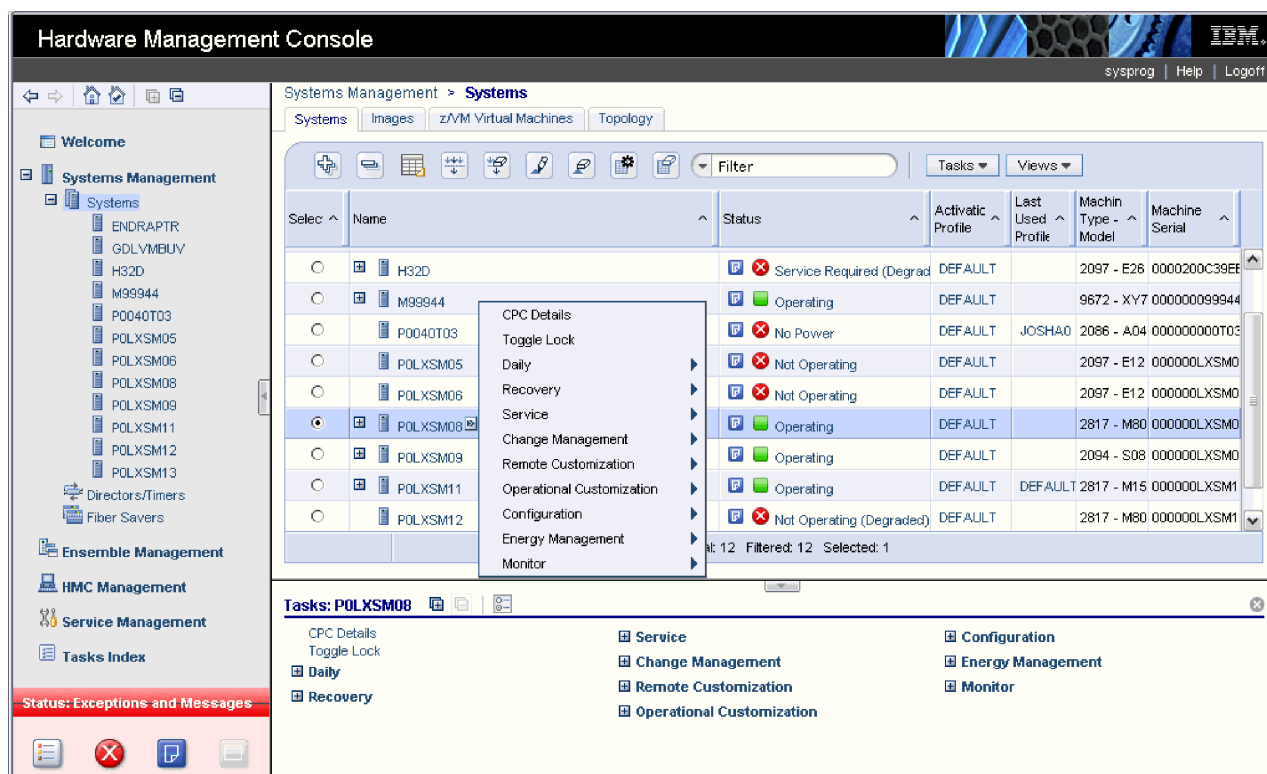


Figure 19. Context menu

Tasks menu: The **Tasks** menu is displayed on the work pane table toolbar, as shown in Figure 20 on page 25. The tasks menu is available only for table selections. For example, in the **Select** column of the Systems 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.

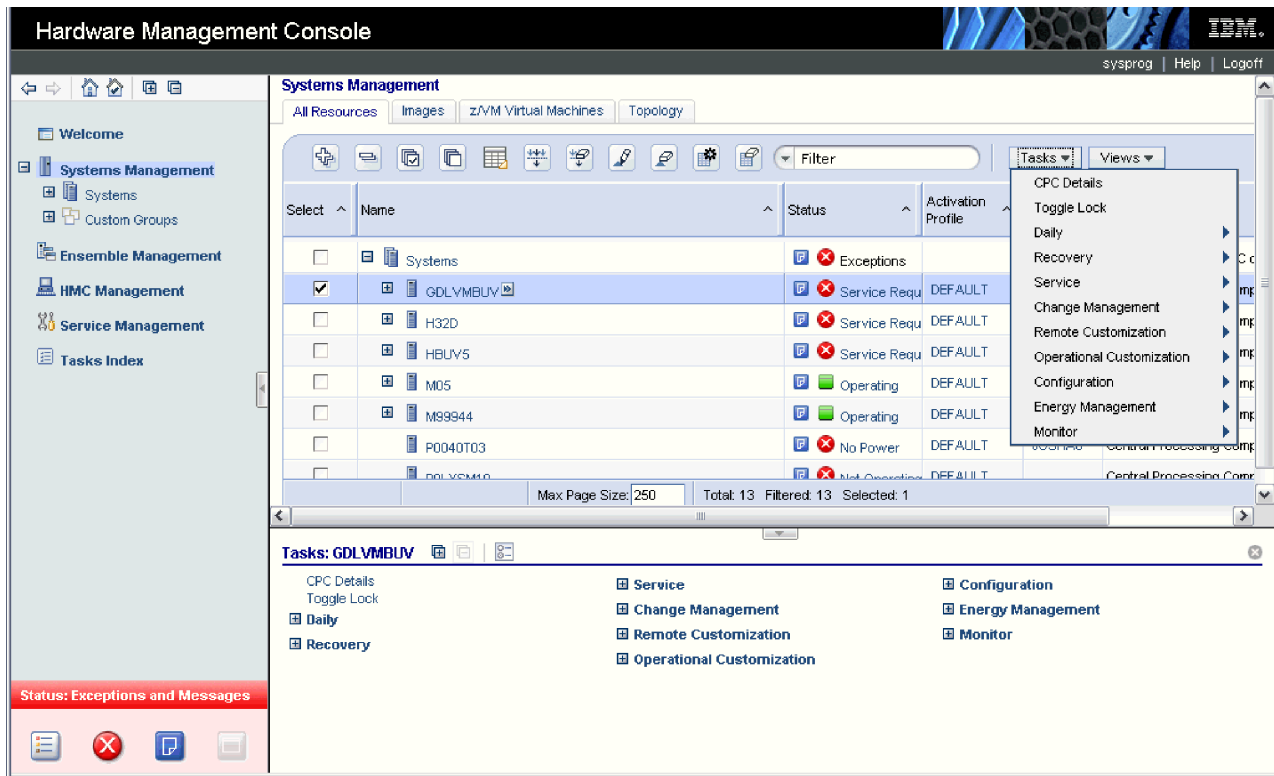


Figure 20. Tasks menu

Additional information from the Systems work pane table includes:

- Status
- Displaying server details
- System images
- z/VM virtual machines.

Status: The **Status** column of the Systems work pane table displays the current status of the server. 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. You can see a sample of the status icons in the **Status** column in Figure 20.

Displaying system details: All system details can be displayed by using one of the following methods:

- Click on 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, as described in “Object locking for disruptive tasks” on page 54, or by clicking on **Toggle Lock** in the tasks pad or from the context menu.

The Systems work pane table includes additional information about the servers 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 to customize the information that is displayed in the work pane table (see “Views menu” on page 41 for more information).

System images: If images are defined for a particular system then they are displayed in the system work pane under the **Images** tab. The contextual tasks associated with a particular image are displayed in the tasks pad. You can also view the images associated with a system by selecting a system in the navigation pane so that the images are displayed in the work pane table under the **Images** tab (see Figure 21).

You can open tasks on the images the same way you open them on the systems. See “Opening tasks for the system” on page 21 for more information.

To display details about an image from the Systems work pane table you can:

- Click on the server image name from the **Name** column, or
- Click in the **Select** column next to the system image name to either:
 - Click **Image Details** in the tasks pad, or
 - Click on the arrow icon next to the image name and select **Image Details** from the context menu (see Figure 21), or
 - Right click on the table cell of the image name and select **Image Details** from the context menu.

In all cases the image Details window is displayed.

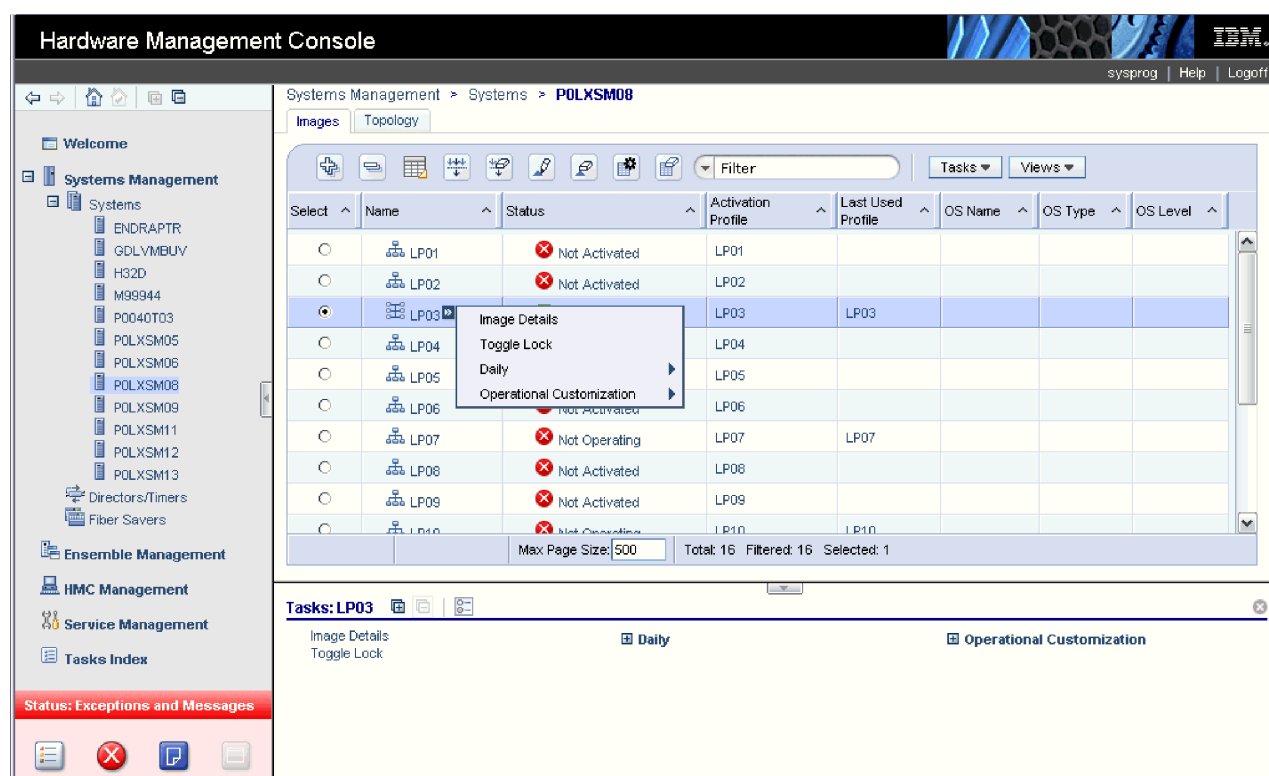


Figure 21. Systems management images window

The images work pane table includes additional information about the images such as the activation profile name, last profile the image used, the operating system name, type, and level for the image.

You can use the **Views** menu to customize the information that is displayed in the work pane table (see “Views menu” on page 41 for more information).

z/VM virtual machines: The **z/VM Virtual Machines** tab, as shown in Figure 21, can be used to display all managed z/VM virtual machines across all images running z/VM 5.3 or later.

Figure 22 is an example of a server image running a z/VM virtual machine. The tasks pad displays the appropriate tasks that can be performed on a selected z/VM virtual machine(s). For more information, see “z/VM Virtual Machine Management” on page 194.

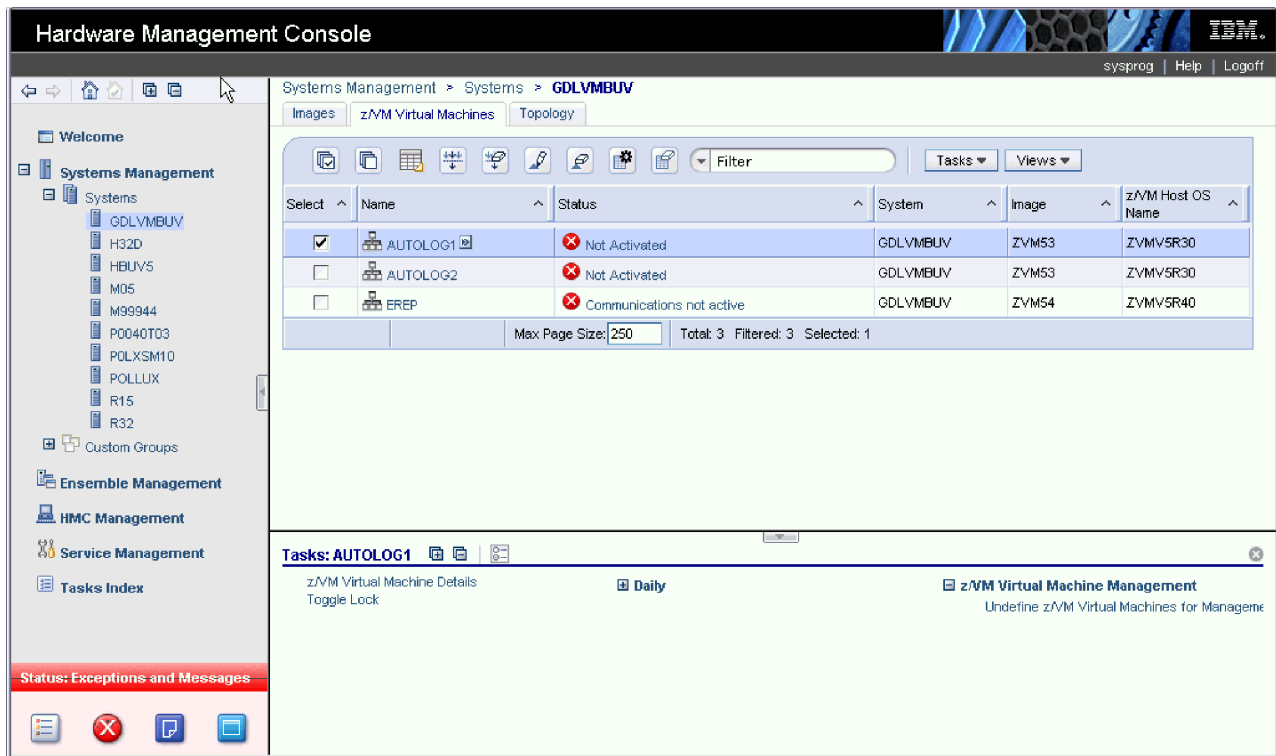


Figure 22. z/VM virtual machines

Directors/Timers

The **Directors/Timers** node represents either an ESCON Director console or a Sysplex Timer[®] console defined to the Hardware Management Console.

This group contains all directors/timers defined to the Hardware Management Console that were either automatically discovered or defined by using the Directors/Timers Definition Template. This group does not display until you have defined a directors/timers object. For more information on defining directors/timers to the Hardware Management Console, see “Directors/timers” on page 29.

Fiber Savers

The **Fiber Savers** node represents the 2029 Fiber Savers defined to the Hardware Management Console.

This group contains all 2029 fiber savers defined to the Hardware Management Console using the Fiber Saver Definition Template. This group does not display until you have defined a fiber saver object. For more information on defining 2029 fiber savers to the Hardware Management Console, see “Fiber savers” on page 29.

The Hardware Management Console will continuously monitor the status of defined fiber saver devices, and if configured to do so, will automatically report fiber saver problems to the IBM Service Support System (RETAIN[®])

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 messages overlay icon is displayed indicating that both messages exist.

User-defined groups: You can use the **Grouping** task under the Daily task group on the tasks pads 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 you can:

1. Select one or more objects that you want to include in the group you want to work with.
2. Open the **Grouping** task from the Daily tasks pad. The Manage Groups window is displayed.
3. From the Manage Groups window, select **Create a new group**, specify a group name and description, click **OK** to complete.
4. 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 or Systems Management tasks pad. The Create Pattern Match Group window is displayed.
2. From the Create Pattern Match Group window, select one or more 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** on the Create a New Group window to complete.
3. The new user-defined group is displayed in the navigation pane under the **Custom Groups** 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.

Unmanaged Resources

The **Unmanaged Resources** node represents the systems, directors/timers, and fiber savers that are not defined to the Hardware Management Console.

Note: The **Unmanaged Resources** node is available only if your user ID is based on the access administrator or service representative task roles.

Systems:

The **Systems** listed under **Unmanaged Resources** are the servers that:

- Are physically installed
- Have their Support Element powered on
- Have the same domain name and domain security as the Hardware Management Console
- Are not managed by your Hardware Management Console.

A server in this group must be defined before tasks can be performed on it. Status is not reported for objects in the Unmanaged Resources Systems group. To define servers, use the **Add Object Definition** task:

1. Select a server by clicking in the **Select** column of the Unmanaged Resources work pane table.
2. Open the **Add Object Definition** task from the tasks pad. The Add or Change Object window is displayed.
3. Click **Save** to add the server to the group of managed servers.

In addition, this group also contains **CPC Manual Definition**. Local Hardware Management Consoles can automatically detect the presence of Support Elements and automatically set up all the necessary internal configuration information for communication without additional information from the users. For remote Hardware Management Consoles, users must provide additional addressing information to perform this configuration.

Use **CPC Manual Definition** to define a server when TCP/IP connectivity exists between the Hardware Management Console and the server:

1. Select **Unmanaged Resources** from the navigation pane.
2. Select **Systems** from the navigation pane or from the Unmanaged Resources work pane table.
3. Open the **Manual Add Object Definition** task from the Systems task pad. The Manual Add Object Definition window is displayed.
4. Specify the TCP/IP address in the **Addressing Information** input field and click **OK**. The Hardware Management Console tries to contact the Support Element and exchange the remaining information necessary to complete the configuration process.

Note: The Manual Add Object Definition window remains displayed with the last entered TCP/IP address until you have added the appropriate servers. When you have completed this task, click **Cancel**.

After a server is defined, it is removed from the **Unmanaged Resources** node and added to the **Systems** node under the **Systems Management** node in the navigation pane. From the **Systems** node, the server can be grouped into one or more user-defined groups. A defined server will remain as part of **Systems** until its definition is removed, regardless of its power state.

Directors/timers:

The **Directors/Timers** listed under **Unmanaged Resources** contains director/timer consoles, if any, that can be defined to the Hardware Management Console but currently are not defined to it. The group also contains a task and template for manually identifying and defining director/timer consoles that the Hardware Management Console cannot automatically discover.

Undefined director/timer consoles and the Director/Timer Console Manual Definition Template can be targets of the **Add Object Definition** task only. To define director/timer consoles, use the **Add Object Definition** task.

To define director/timer consoles:

1. Select the **Unmanaged Resources** node from the navigation pane.
2. Select the **Directors/Timers** node from the navigation pane or Unmanaged Resources work pane table.
3. Open the **Manual Add Object Definition** task from the directors/timers tasks pad. The Director/Timer Console Manual Add Object Definition window is displayed.
4. Enter the **TCP/IP address**, then click **Find** to locate the TCP/IP address.
5. If you get the message that the director/timer console was contacted, click **Save** to add the director/timer console.
6. After the director/timer console is added, click **OK**. The director/timer console is now added to the **Directors/Timers** node under the **Systems Management** node in the navigation pane.

Fiber savers:

This system-defined group contains a template for manually identifying and defining 2029 fiber savers. Undefined Fiber Savers and the Fiber Saver Manual Definition Template can be targets of the **Add Object Definition** task only.

To define fiber savers:

1. Select the **Unmanaged Resources** node from the navigation pane.
2. Select the **Fiber Savers** node from the navigation pane or work pane table.
3. Open the **Manual Add Object Definition** task from the Fiber Savers tasks pad. The IBM Fiber Saver (2029) Manual Add Object Definition window is displayed.
4. Enter the **TCP/IP address** and the **Community name**.
5. Click **Find**.
6. If you get the message that the fiber saver was contacted, click **Save** to add the fiber saver.
7. After the fiber saver is added, click **OK**. The fiber saver is now added to the **Fiber Savers** node under the **Systems Management** node in the navigation pane.

Ensemble Management



Ensemble Management manages systems in an Ensemble. When you select **Ensemble Management** from the navigation pane, the work pane initially displays a **Getting Started** tab that explains how to set up and manage an ensemble. Use the **Ensemble Management Guide** task to assist you with setting up and managing an ensemble.

Note: When an ensemble has been created, the Getting Started page is no longer displayed in the work pane.

You can see the *Hardware Management Console Guide for Ensembles* for more detailed ensemble information. A link is provided on the **Getting Started** tab.

HMC Management



HMC Management allows you to perform tasks associated with the management of this console. When you select **HMC Management** from the navigation pane the work pane contains a view of the Hardware Management Console tasks and their descriptions. These tasks are used for setting up the Hardware Management Console, maintaining its internal code, and securing the Hardware Management Console. Most likely, you will not use these actions on a regular basis.

To see what level of the Hardware Management Console you are currently working with, point your mouse over **HMC Version** found at the top of the work pane.

To display the tasks in the work pane:

1. Select the **HMC Management** node in the navigation pane.
2. By default, a categorized listing of the tasks is displayed. The tasks are arranged in groups which include:
 - Security
 - Configuration.
3. From the work pane, click on the task you want to perform.

If you want an alphabetical 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** views you can also choose:

- **Detail** displays the tasks in the original tree style user interface style with a small task icon followed by the task name and description in two columns.
- **Icon** displays large task icons above the task name, similar to the classic style user interface task display.
- **Tile** displays tasks using large icons followed by task names and descriptions to help you find tasks by icon while still providing task descriptions.

See Figure 23 for an example of an alphabetical sort of the HMC management tasks using the icon style.

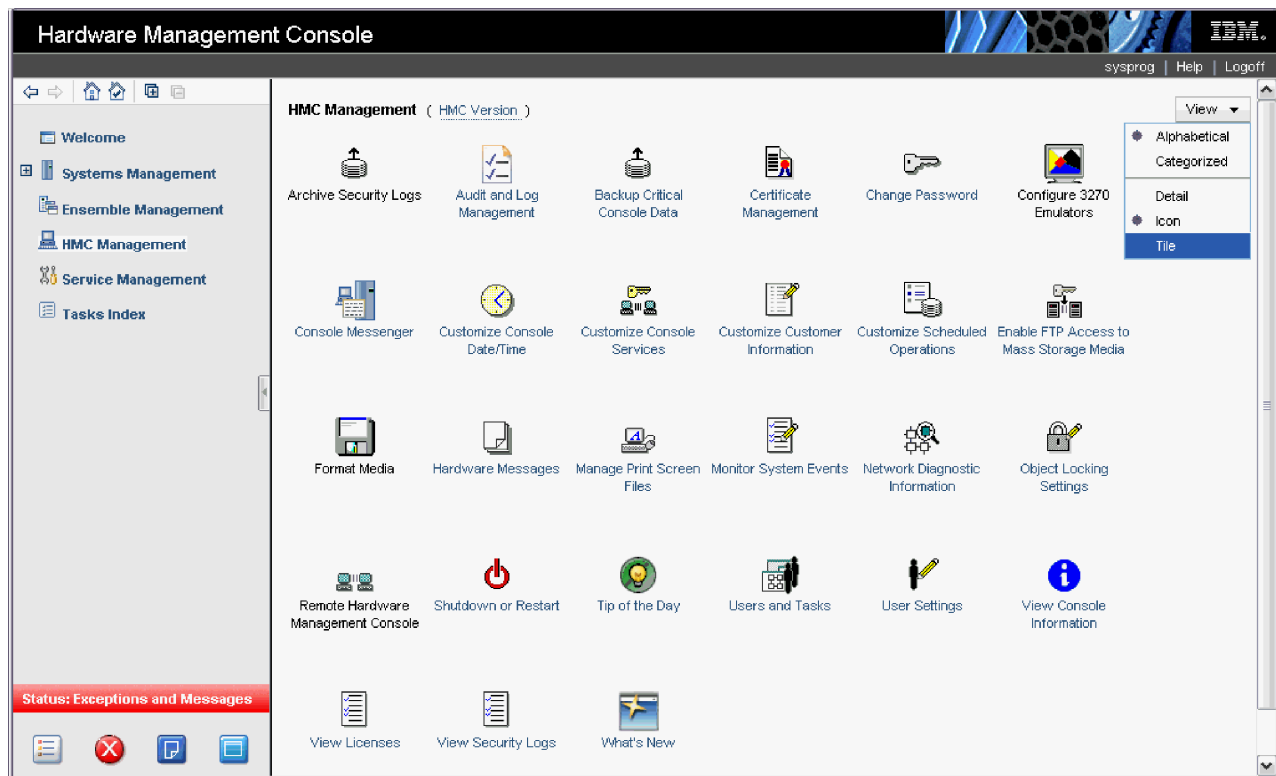


Figure 23. Tasks using an alphabetical sort with icon style

The following HMC management tasks, in alphabetic order, are displayed in the work pane depending on the task roles defined to your user ID. They are described in further detail in Chapter 5, “Hardware Management Console tasks,” on page 81.

Note: Some tasks cannot be opened if you are accessing the Hardware Management Console remotely.

- Archive Security Logs
- Audit and Log Management
- Backup Critical Console Data
- Certificate Management
- Change Password
- Configure 3270 Emulators
- Configure Data Replication
- Console Default User Settings
- Console Messenger
- Create Welcome Text
- Customize API Settings
- Customize Automatic Logon
- Customize Console Date/Time

- Customize Console Services
- Customize Customer Information
- Customize Network Settings
- Customize User Controls
- Customize Scheduled Operations
- Domain Security
- Enable FTP Access to Mass Storage Media
- Format Media
- Hardware Messages
- Manage Enterprise Directory Server Definitions
- Manage Print Screen Files
- Manage SSH Keys
- Manage Users Wizard
- | • Manage Web Services API Logs
- Monitor Systems Events
- Network Diagnostic Information
- Object Locking Settings
- Password Profiles
- Remote Hardware Management Console
- Save/Restore Customizable Console Data
- Save Upgrade Data
- Shutdown or Restart
- Tip of the Day
- User Profiles
- Users and Tasks
- User Patterns
- User Settings
- User Templates
- View Console Information
- View Licenses
- View Security Logs
- What's New

Service Management



Service Management allows you to perform tasks associated with servicing this console. When you select **Service Management** from the navigation pane the work pane contains a view of the service management tasks and their descriptions. These tasks are used to service the Hardware Management Console and maintain its internal code.

To see what level of the Hardware Management Console you are currently working with, point your mouse over **HMC 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. By default, a categorized listing of the tasks is displayed. The tasks are arranged in groups which include:
 - Console Logs
 - Console Internal Code
 - Configuration.
3. From the work pane, click on the task you want to perform.

If you want an alphabetical 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** views you can also choose:

- **Detail** displays the tasks in the original tree style user interface style with a small task icon followed by the task name and description in two columns.
- **Icon** displays large task icons above the task name, similar to the classic style user interface task display.
- **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.

See Figure 24 for an example of a categorized view of the service management tasks using the tile style.

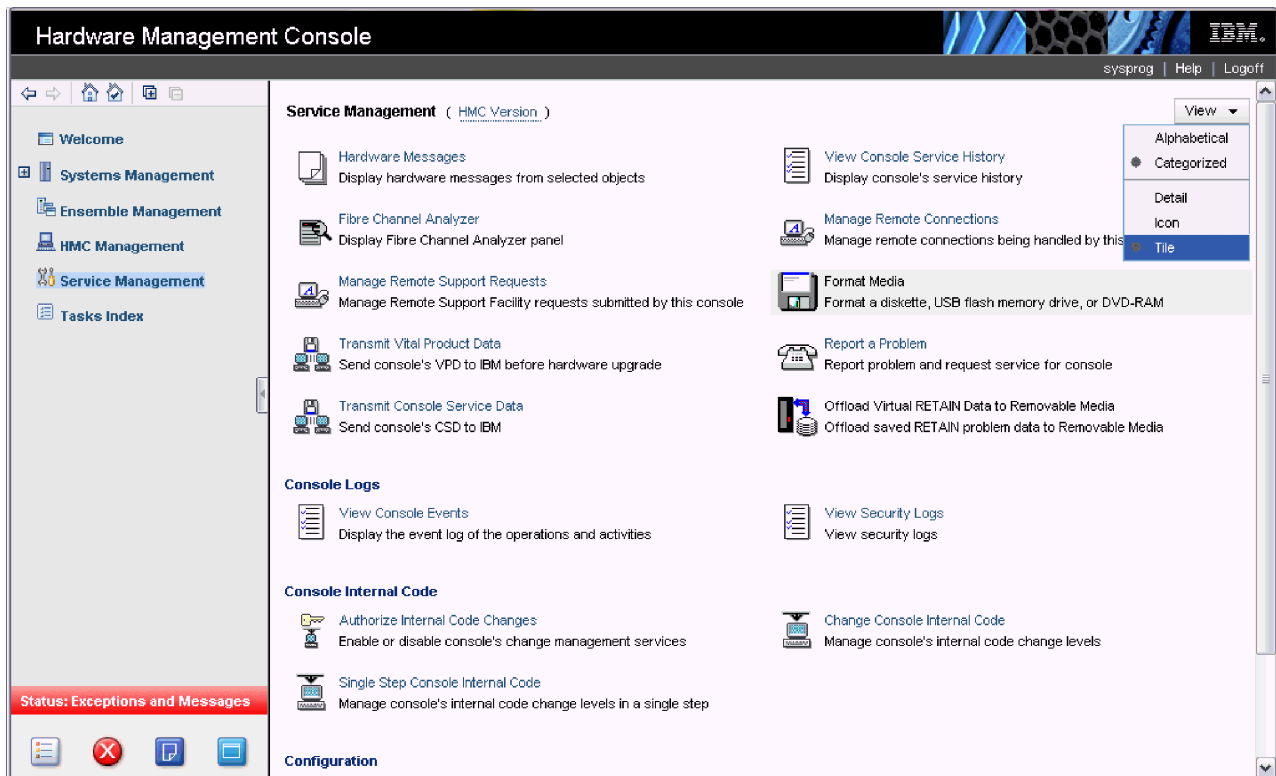


Figure 24. Tasks using a categorized sort with tile style

The following Service Management tasks, in alphabetic order, are represented in the work pane depending on the task roles defined to your user ID. They are described in further detail in Chapter 5, “Hardware Management Console tasks,” on page 81.

Note: Some tasks cannot be opened if you are accessing the Hardware Management Console remotely.

- Analyze Console Internal Code
- Authorize Internal Code Changes
- Block Automatic Licensed Internal Code Change Installation
- Change Console Internal Code
- Copy Console Logs to Media
- Customize Auto Answer Settings
- Customize Modem Settings
- Customize Outbound Connectivity
- Customize Product Engineering Access

- Customize Remote Service
- Enable Electronic Service Agent™
- Fibre Channel Analyzer
- Hardware Messages
- Installation Complete Report
- Manage Remote Connections
- Manage Remote Support Requests
- Offload Virtual RETAIN Data to Removable Media
- Perform a Console Repair Action
- Reassign Hardware Management Console
- Rebuild Vital Product Data
- Report a Problem
- Restore Legacy HMC Data
- Single Step Console Internal Code
- Transmit Console Service Data
- Transmit Vital Product Data
- View Console Events
- View Console Service History
- View Console Tasks Performed
- View PMV Records
- View Security Logs

Tasks Index



Tasks Index allows you to select and perform a task 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. 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 **HMC 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 is located 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 **HMC 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 can be reset back to zero by clicking **Tasks** from the work pane table toolbar, then selecting **Reset Task Launch Count** (see Figure 25).
- 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” on page 39 for more detailed information about using the icons and the quick filter function.

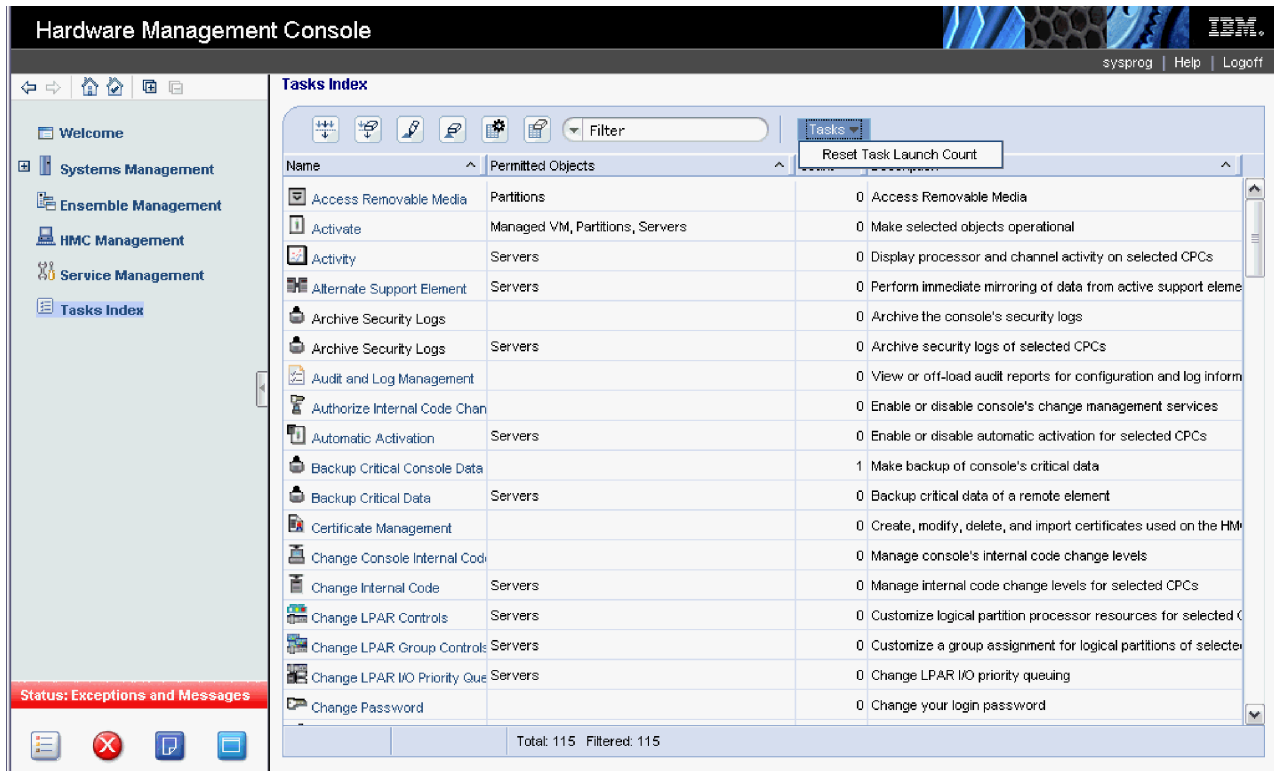


Figure 25. Tasks index

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 a **Systems Management** work pane.

Selecting an object from the navigation pane displays a resources (configurable) table in the work pane as shown in Figure 26 on page 36. 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.

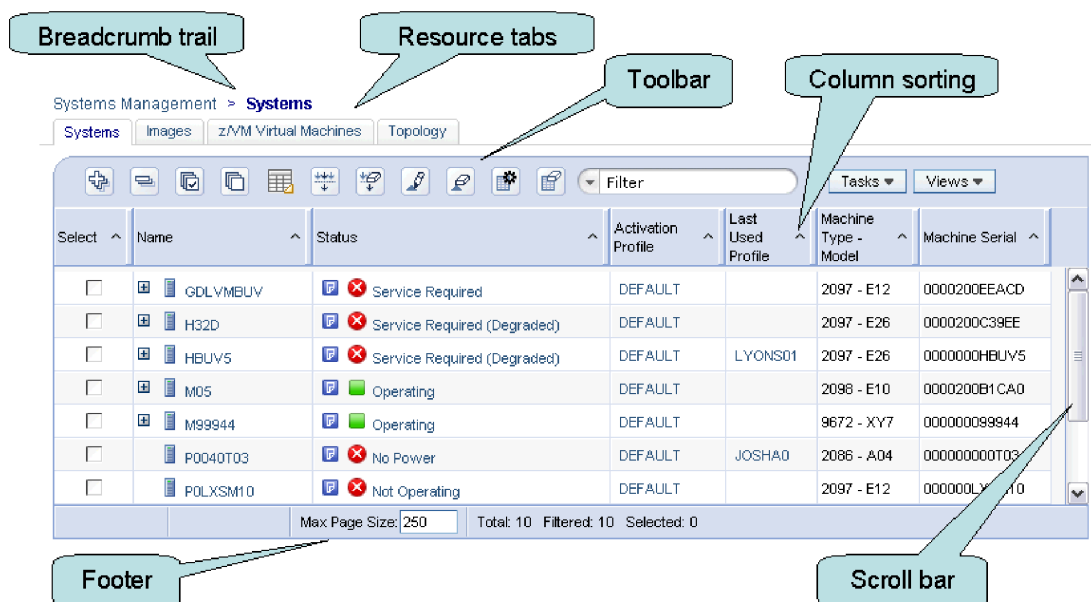


Figure 26. Work pane table features

Work pane table

The information that is displayed in the work pane table allows you to view an object and its children in the same 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” on page 39 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 located 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 the object.

You can customize these tables using the **Manage Views** option from the **Views** menu, see “Creating a custom work pane table view” on page 37.

For an example of the work pane table, see Figure 27 on page 37.

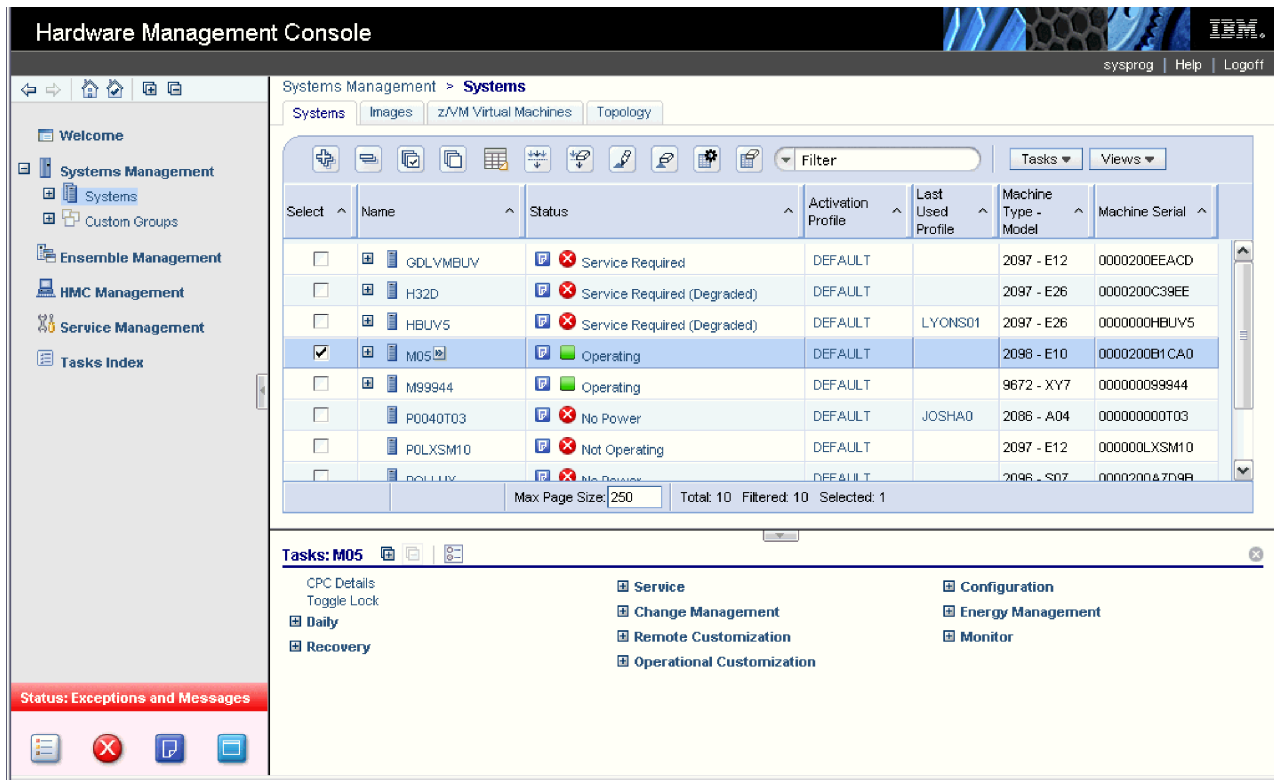


Figure 27. System management work pane table

You can also reorder the columns of the 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.

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 the **Views** menu.

Note: The settings that you define within the tree style user interface are saved when you log off the Hardware Management Console.

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 is located above the resources table.
3. You can specify a unique name for your custom view in the **View Name:** input field (see Figure 28 on page 38).
4. Select the items 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.

- 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.

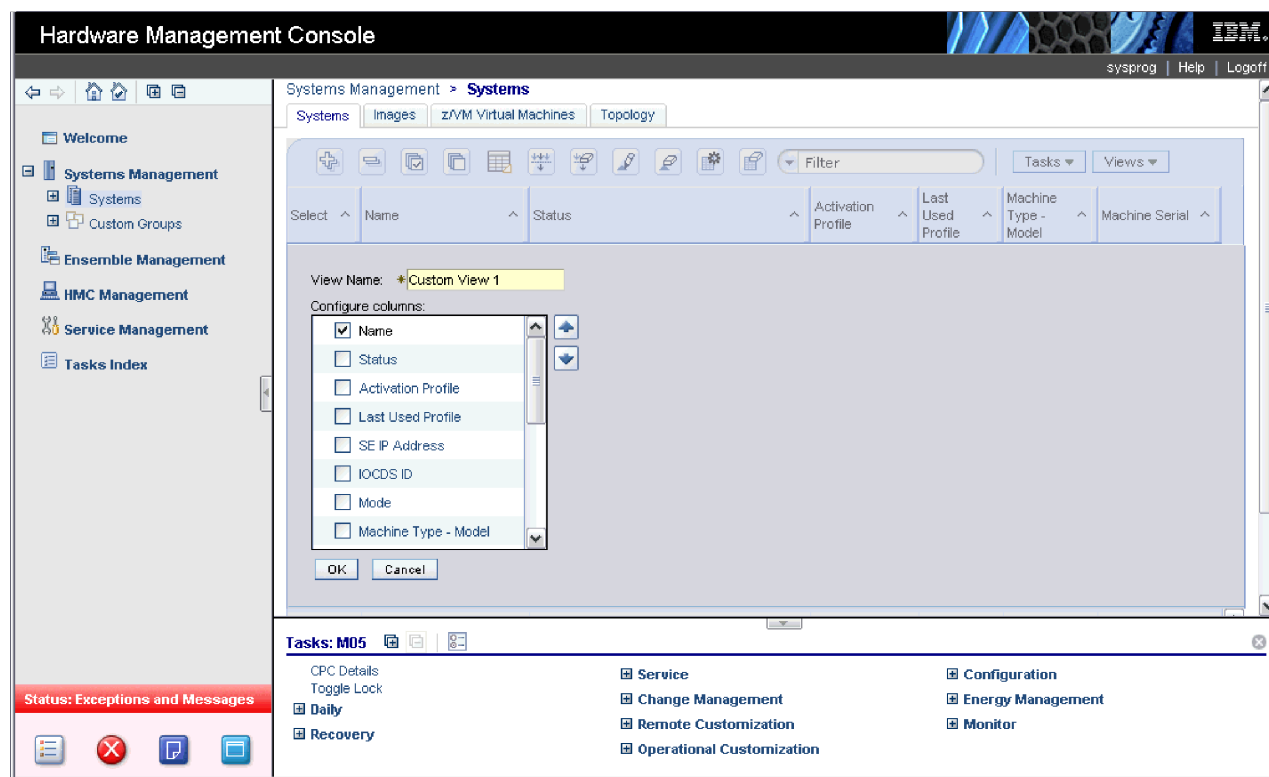


Figure 28. Custom table view

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 is displayed 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 delete from the **Custom Table Views** list.
3. Click **Delete** in the **Manage Views Dialog**.
4. If a confirmation panel is displayed, 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 Systems 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. Figure 26 on page 36 shows an example of this information.

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 Systems Management work pane table contains icons used to expand, collapse, export, 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.

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.

Note: These icons are displayed only if you have chosen to select multiple objects. To set the object selection mode use the **User Settings** task.

Export data



The **Export Data** icon allows for table data to be downloaded in a Comma Separated Values (CSV) file. This downloaded CSV file can then be imported into most spreadsheet applications.

Note: This function is available only when you are accessing the Hardware Management Console remotely.

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.

Note: When you are filtering within the work pane table the objects cannot be expanded.

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.

Note: When you are sorting within the work pane table the objects cannot be expanded.

Column configuration



Use the column configuration buttons to manage the columns displayed in the Systems 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.

Note: When you are sorting or filtering within the work pane table the objects cannot be expanded.

Tasks menu

The **Tasks** menu is displayed on the work pane table toolbar and is only available for table selections when working with managed objects and custom groups. See “Tasks menu” on page 24 for more information.

Views menu

The **Views** menu is displayed on the work pane table toolbar when working with managed objects and custom groups. This menu allows you to display different sets of attributes (columns) in the table. Figure 29 shows an example of the **Views** options when you are working with servers.

For information on defining your own table view, see “Creating a custom work pane table view” on page 37.

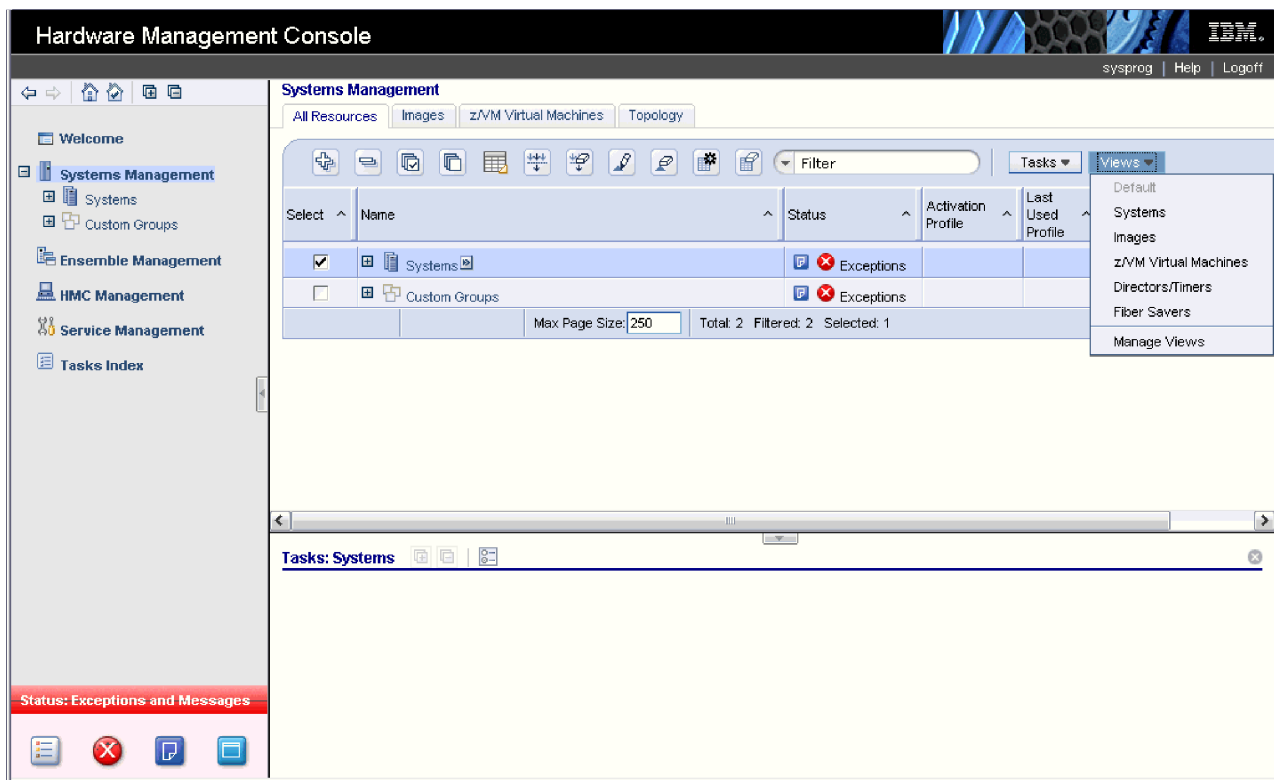


Figure 29. Systems views menu

Topology

The information that is displayed from the **Topology** tab is a graphical relationship-based view of the objects. It is composed of the Toolbar, Framed image, and Support areas, some of which are identified in Figure 30 on page 42.

Note: When an object's status changes or new objects have been added or removed, the image is updated and the new content automatically fits in the current work pane area.

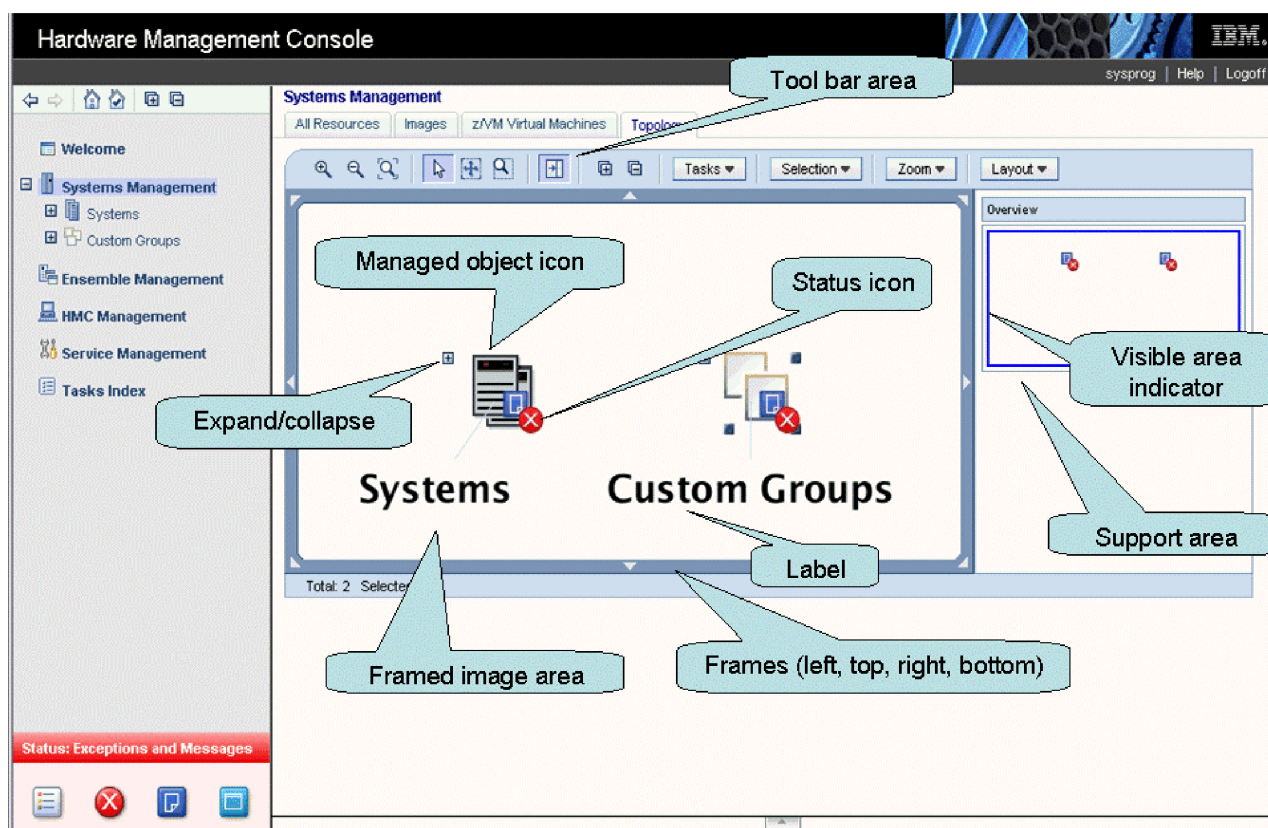


Figure 30. Topology view features

Toolbar

This area of the topology work pane consists of several icons and drop-down menus for controlling the appearance and actions of the topology view. You can mouse over the toolbar icons for short descriptions of the respective actions.

The toolbar icons are divided into the following groups:

- Content zoom and fit control - used for enlarging and shrinking the images and automatically fitting the image content within the work pane area:
 - **Zoom In**
 - **Zoom Out**
 - **Fit Contents to Viewport**
- Mouse modes - controls the function of the mouse.
 - **Select Mouse Mode** (default) - clicking on an object causes its selection to be toggled.
 - When a node is selected, the tasks context menu icon is displayed and the tasks in the **Tasks** menu are also updated.
 - When multiple selection is enabled, press (Ctrl +) left mouse button to select multiple nodes. Left clicking in a blank area of the work pane area deselects all selected nodes.
 - **Pan Mouse Mode** - scroll the objects in the frame up, down, left, or right using direct manipulation. After you release the mouse button, the mouse mode is automatically changed back to the selection mode.

- **Zoom Mouse Mode** - creates a viewport to zoom into. The mouse is used to select a rectangular area (a blue box is displayed to indicate the area) as part of the image frame to zoom into. The objects in the area are enlarged. After you release the mouse button, the mouse mode is automatically changed back to the selection mode.
- Toggle Support Area Visibility icon - toggles the visibility of the support area, which displays the image Overview (see Figure 30 on page 42).
- Expand All / Collapse All icons - expand (display) or collapse (hide) the children of all objects.

The drop-down menus include:

- **Tasks** - when one or more objects are selected the tasks available for the objects are displayed. These same tasks are displayed in the context menu and tasks pad.
- **Selection** - allows you to select all the objects, deselect all the objects, or invert selection.
- **Zoom** - allows you to change the content size:
 - Fit Content**
Automatically fits the objects in the framed image area.
 - 50%** Size of each object is displayed as half its actual size.
 - 100%** Size of each object is displayed as the actual size.
 - 200%** Size of each object is displayed as twice the actual size.
- **Layout** - allows you to select the preferred object layout:
 - Rerun Current**
Redraws the image using the current layout.
 - Tree** Displays objects in a hierarchical tree format.
 - Hierarchical**
Arranges the nodes so that the majority of links are short and flow uniformly in the same direction.
 - Circular**
Objects are automatically grouped into either a ring or star topology.
 - Uniform length**
Searches for a configuration of the graph where the length of the links are the same.
 - Grid** Objects are placed into a grid.

Framed image

This area displays graphical representations of managed objects. Each object is represented with a graphic which displays the object's name, its status, its tasks (in a context menu), and an expand/collapse button if it has children. Note some of the following characteristics as you work in the framed image:

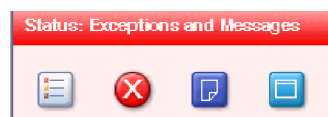
- If an object is selected, the label uses black font color and blue background color, the background of the object icon also turns blue.
- The status icon overlay is a combination of the system status icon, hardware messages icon, and the operating system messages icon.
- If an object is locked, the lock icon is displayed.
- If an object is busy, the busy icon is displayed.
- Click on a frame segment to redraw the image that has been panned in the associated direction.
- Click the right mouse button in an empty area of the images frame to display a context menu with the following additional options (similar to the Toolbar functions):
 - **Collapse All**
 - **Expand All**
 - **Selection**
 - **Zoom**
 - **Layout**
 - **Center here** - centers you on the current mouse position.
 - **Move here** - moves the selected object into the current mouse position (this option displays only when exactly one object is selected).

- Click the right mouse button or click the double arrow icon on a selected object to display a context menu with the following additional options:
 - **Zoom To** - zooms into the object in the center of the viewer display area.
 - **Center here** - centers you on this object.
 - **Expand** - expands the object by displaying any children if an object is collapsed.
 - **Collapse** - collapses the object by hiding its children if an object is expanded.

Support

This optional area (click **Toggle Support Area Visibility** icon on the toolbar) is used to display a high level view of the topology of the entire system configuration with only the status of managed resources represented. Moving the rectangle changes what is displayed in greater detail in the image viewer area.

Status bar



The status bar, in the bottom left pane, provides an "at a glance" view of overall system status, including managed system resources and the Hardware Management Console. A status-sensitive title, background color, and icons are part of the status bar. The Status Overview icon is always available in the status bar. Indicators (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 Exceptions icon to view all resources with an exception state. The results are displayed in a table in the work pane.

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 or the Hardware Management Console receives a hardware message, the Hardware Message indicator (icon) displays 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 that displays 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 opens. Now you can work with your messages.

Operating System Messages



If a managed object receives an operating system message, the **Operating System Message** indicator (icon) displays 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 that is displayed 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 opens. 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, as shown in Figure 31. 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.

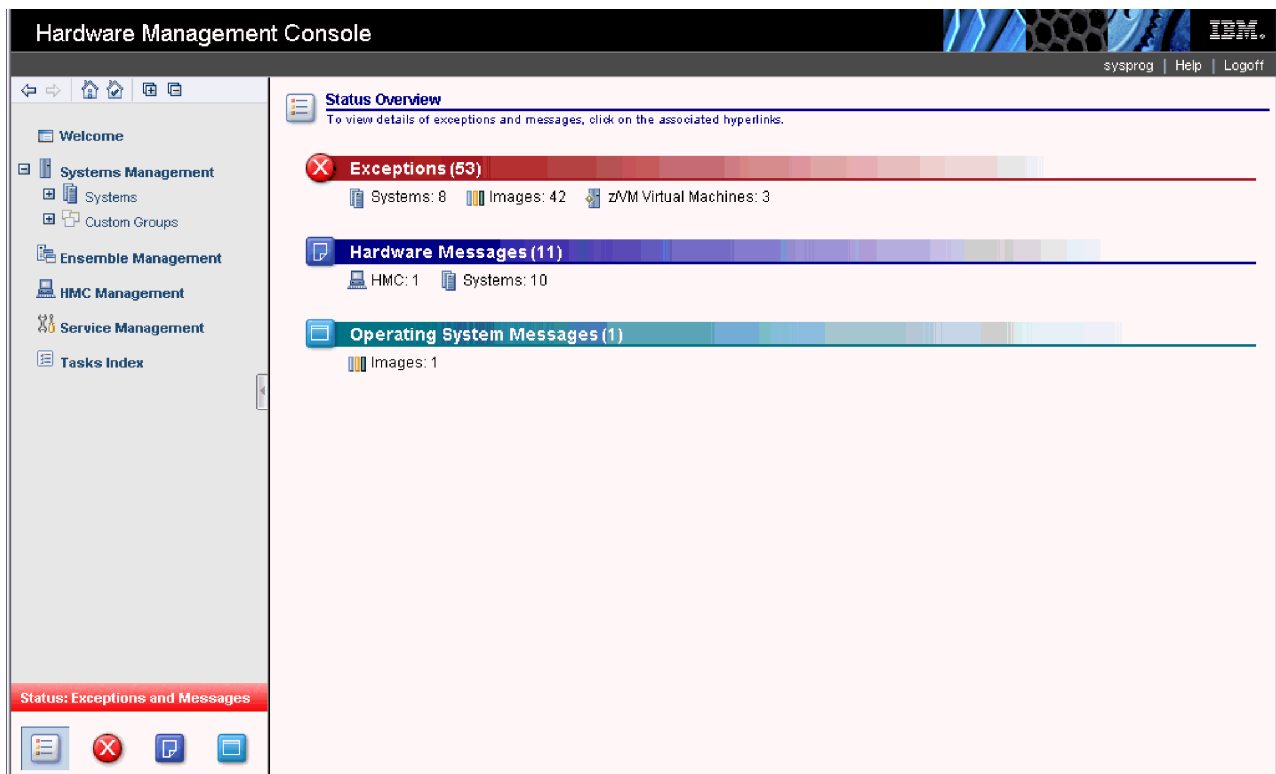


Figure 31. Status overview

Object locking for disruptive tasks

You can tell when a system or system image is locked because a small lock is displayed next to the system name in the work pane table. In the topology view the icon is shown as an overlay of the object icon.



The setting of a server or server image's toggle lock determines whether you can perform a disruptive task on the server or server images. You can lock an individual object or automatically lock all objects.

To individually lock (or unlock) a server or server image:

1. Select the server from the table that you want to lock (or unlock).
2. Click **CPC Details** from the tasks pad. The CPC Details window is displayed.
3. You can select **Yes** or **No** for **Lock out disruptive tasks**.
4. Click **Apply** to make the change.

An alternate way to lock (or unlock) an individual object is to:

1. Select the object from the table that you want to lock (or unlock).
2. Click **Toggle Lock** from the tasks pad.

To lock (or unlock) more than one server or server image:

1. You must have multiple selections enabled from the **Controls** tab of the **User Settings** task.
2. Select all the servers from the table that you want locked (or unlocked).
3. Click **Toggle Lock** in the tasks pad.
4. The icons in the table will change to either a server icon or a small lock icon, depending on what action you want to perform on that server or server image.

There is also an automatic way to lock the all the servers and server images 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 Hardware Management Console.

1. Open the **Object Locking Settings** task from the **HMC Management** work pane. The Locking window opens.
2. Select **Automatically lock all managed objects** or **Relock after a task has been run** or both.

Chapter 4. Using the classic style user interface

This chapter explains how to use the classic style user interface for performing tasks on the Hardware Management Console or on a selected CPC or group of CPCs.

Hardware Management Console workplace

The classic style user interface Hardware Management Console window, as shown in Figure 32, consists of three main areas: a *Views* area, a *Tasks* area, and a *Work* area.

The *Views* area, in the upper left portion of the window, contains icons that represent different collections or views of the objects that make up your system. The background color of this area also gives an indication of the status of the system, as described in “Monitoring your hardware” on page 55.

The *Tasks* area, in the right portion of the window, contains icons that represent the operations that you can perform on the objects.

The *Work* area, in the lower left portion of the window, is the area of the window that displays either objects or groups, tasks in progress, task lists, tasks for monitoring your Hardware Management Console, or the online books, based on the view that you select. Initially, the objects of the **Groups** view are displayed in the *Groups Work Area* as shown in Figure 32.

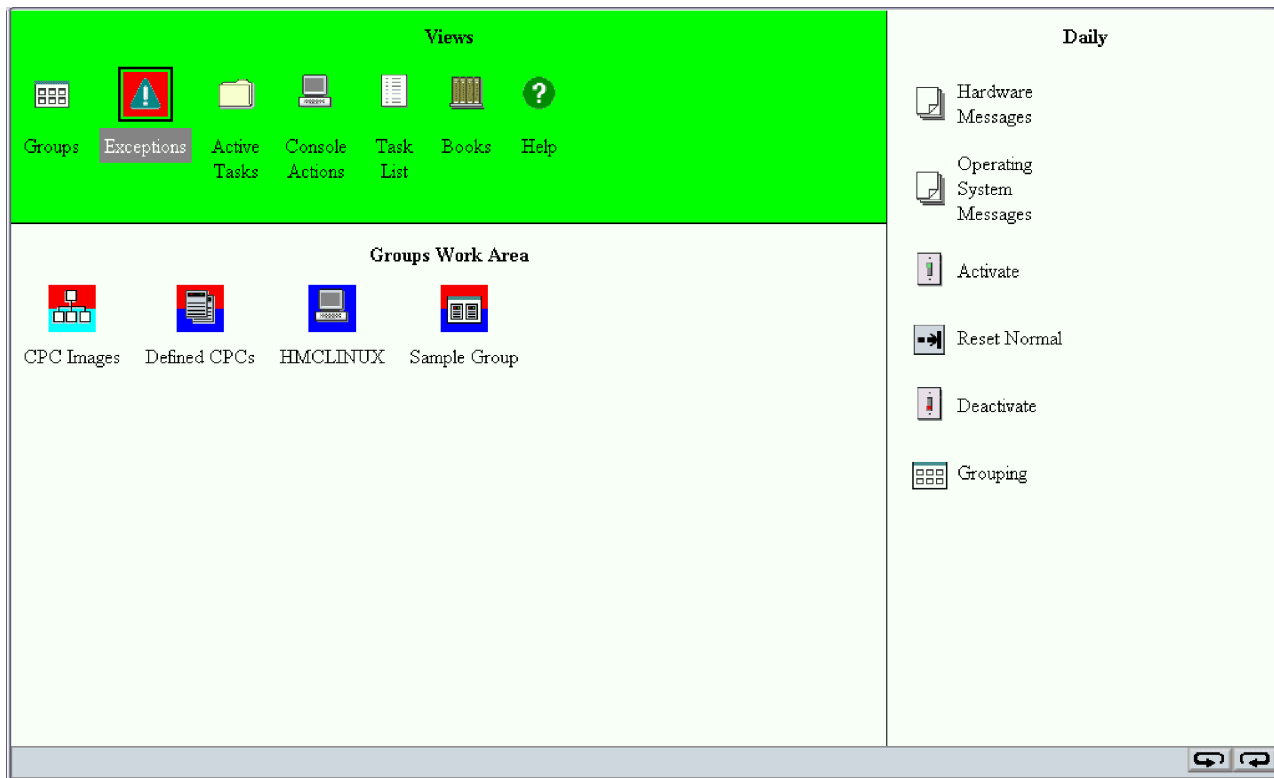


Figure 32. Classic style user interface Hardware Management Console workplace window

You can resize these three areas of the Hardware Management Console workplace. For example, if you are currently working in the *Tasks* area and need additional space to display all of the available tasks, move the mouse pointer over the border that separates the *Tasks* area from the *Views* and *Work* area 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. Release the button and your *Tasks* area is now larger in size. You can make each of the three areas either larger or smaller.

Until you become familiar with these three areas and all the objects in the workplace, you may want to use *Online help*, by double-clicking on the **Help** icon from the *Views* area. Online help provides extensive, comprehensive information for each workplace object. For more information on using online help, refer to “Help” on page 80.

As you become familiar with the workplace, you may want to use *hover help* instead. Hover help is a brief description of an object's contents, usage, or purpose. The help is displayed in a compact pop-up window that hovers above the object. You can set hover help either on or off, depending on what you want. Initially, hover help is set off.

To set hover help on for your workplace:

1. Open **Console Actions** from the **Views** area.
2. Open **User Settings** from the **Console Actions Work Area**. The User Settings window is displayed.
3. Select the **Controls** tab on the User Settings window.
4. Select **Show hover help** (a check mark is displayed), click **Apply**, then click **OK** to enable hover help.

Note: Hover help is not displayed immediately. The cursor must remain placed on a workplace object (icon) for several seconds to display the help.

Selecting objects

Selecting objects prepares them for further action. Selecting a Views icon allows you to display the view by pressing **Enter**. The default setting for selecting objects displayed in the *Work* area is **Single object selection**. However, to select more than one object at a time, allowing you to perform tasks on them as a dynamic group, you can do the following:

1. Open **Console Actions** from the **Views** area.
2. Open **User Settings** from the **Console Actions Work Area**. The User Settings window is displayed.
3. Select the **Controls** tab on the User Settings window.
4. Deselect **Single object selection** by clicking on the check mark to remove it, click **Apply**, then click **OK** when you are finished with the task.

In the *Work* area, if the selection of multiple objects is allowed, you can use one of the following methods for selecting multiple objects:

- Click on each object to be selected.
- Select or deselect all objects in a view.

To select all objects:

1. Display the objects you want to select. For example, click **Defined CPCs** so those objects are displayed in the *Work* area.
2. Right-click on a spot on the **Defined CPCs Work Area** without an icon. This displays the menu for the *Work* area (see Figure 33 on page 49).
3. Click **Select all**. This selects all the objects in the *Work* area.

To deselect all objects, if all objects are selected:

1. Right-click on a spot on the **Defined CPCs Work Area** without an icon. This displays the menu for the *Work* area (see Figure 33 on page 49).
2. Click **Deselect all**. This deselects all the objects in the *Work* area.

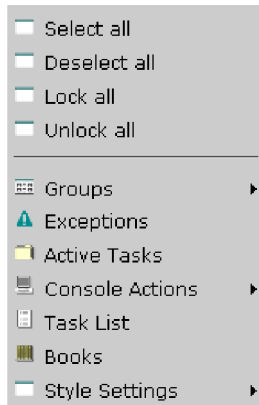


Figure 33. Work area menu

Clicking individual objects that are already selected deselects the objects.

Note: There are times when you only want to work with one object at a time and you want to ensure that additional objects are not accidentally selected. Use the **User Settings** task to verify the **Single object selection** option is selected (a check mark is displayed).

Opening an object

Opening an object in the Work area displays a further level of detail about the object, if available. There are several ways to open an object. One way is to double-click it. Figure 34 on page 50 displays a Groups view including defined CPCs.

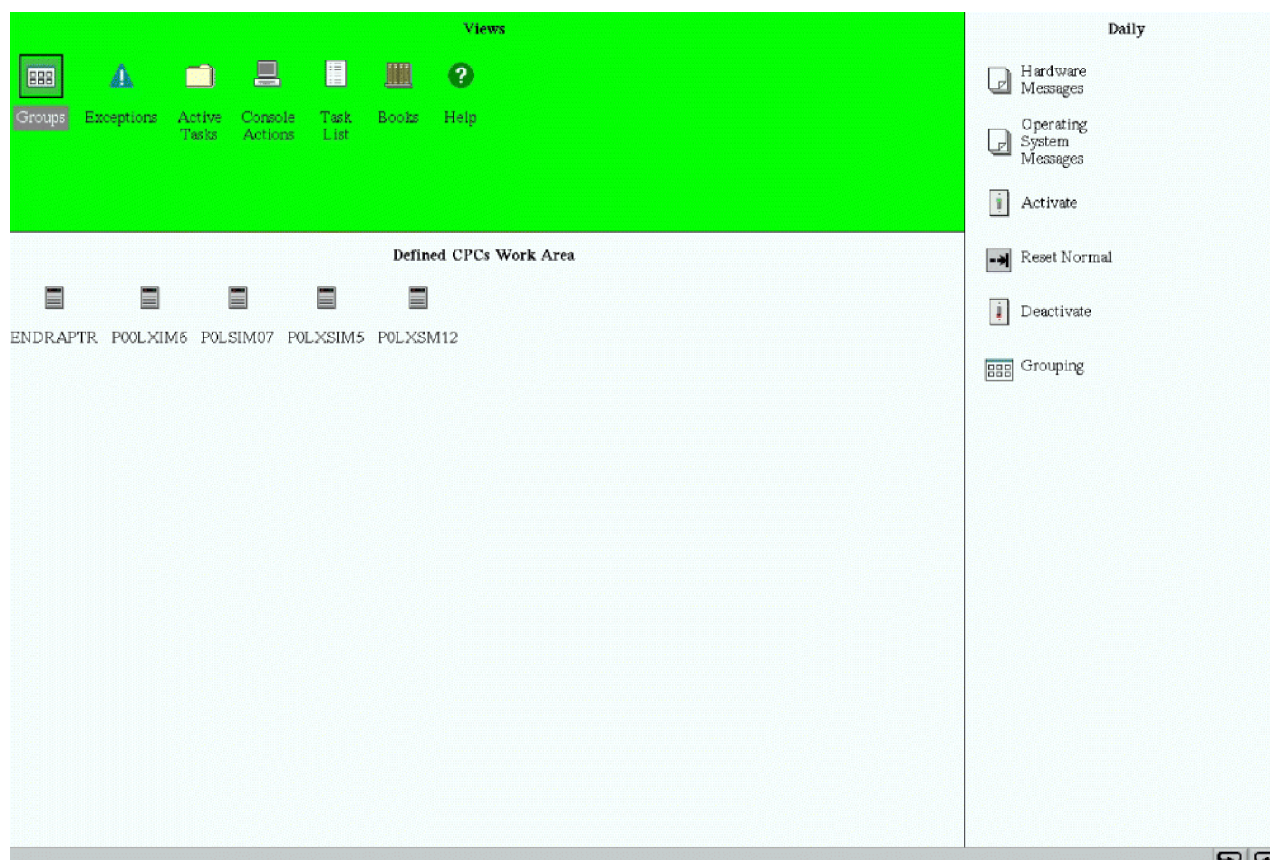


Figure 34. Groups view

Double-clicking any one of the Groups icons in the **Groups** view displays icons for the objects (for example, CPCs or CPC images) that make up that group. Figure 34 shows the objects that make up the **Defined CPCs** group and are displayed in the *Work* area after double-clicking the **Defined CPCs** icon.

Another way to display the icons that make up the group is to right-click the object (such as **Defined CPCs** or **CPC Images**) and, on the menu that is displayed, click **Open**.

Displaying CPC or image details

After you display the objects that make up a group, you can display information about the object in the group (such as a particular CPC or image) by double-clicking it. Then a window opens that displays the object's current status information and other object details.

If you are managing z/VM virtual machines and you want detailed information about z/VM virtual machines, then see “Managed z/VM virtual machines” on page 67.

An alternate way to display this information is to right-click the object's icon and then click **CPC Details** or **Image Details**, respectively. Right-clicking on an object displays its pop-up menu. Figure 35 on page 51 shows the pop-up menu for a CPC.

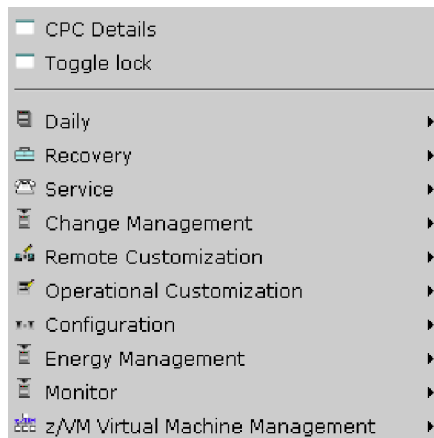


Figure 35. CPC pop-up menu

Selecting **CPC Details** on this menu displays the details about the object. (Refer to “Performing a task on an object” on page 52 for information about clicking the second set of menu items.) Figure 36 shows an example of a CPC Details window.

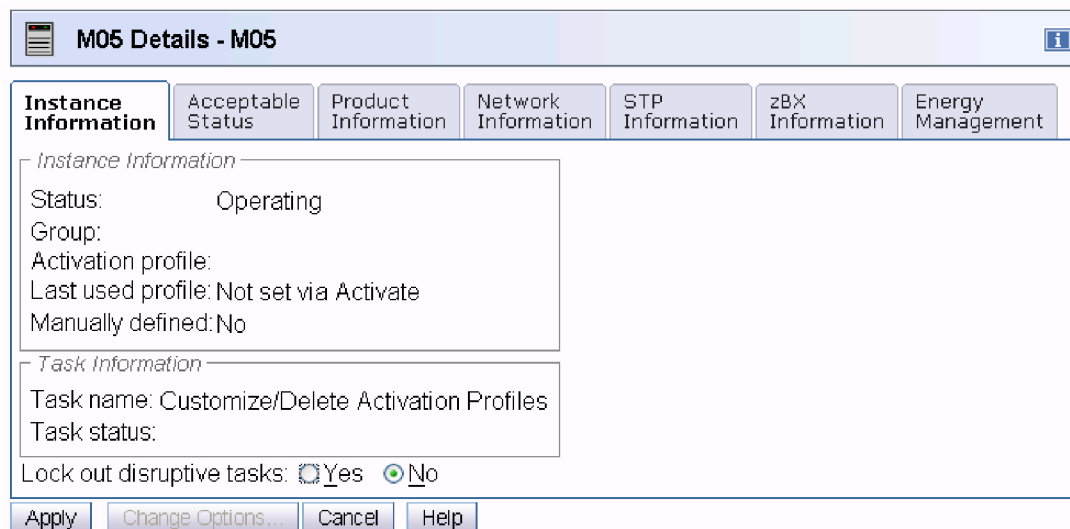


Figure 36. CPC details window

The Details window includes the following tabs:

Instance Information

Includes instance information and task information.

Acceptable Status

Shows the various states and their associated colors and indicates the current state. You can change the acceptable status for all of the current objects that are defined with the same type by selecting **Save as default**.

Product Information

Shows CPC information, machine information, and the software model capacity identifiers.

Network Information

Shows the current network information for the CPC.

STP Information

Shows the current Server Time Protocol (STP) status for the CPC.

Note: This tab is available only when STP is enabled and the selected CPC is in an operating state.

Busy Status

Specifies the reason the CPC object is busy.

Note: This tab is available only when an object is busy. (It can appear for all managed objects including CPCs, images, director/timers, fiber savers, and z/VM virtual machines.)

zBX Information

Specifies the IBM zEnterprise BladeCenter Extension (zBX) information.

Note: This tab is available only when the zBX feature is available for the specified server. For more information on zBX management, see the *Hardware Management Console Operations Guide for Ensembles*.

Energy Management

Specifies power and thermal monitoring information. For more information on energy management, see the *Hardware Management Console Operations Guide for Ensembles*.

Note: Certain information on this tab is available only when the appropriate feature is installed.

The **Lock out disruptive tasks** selection is under the **Instance Information** tab. The **Change Options...** selection is on every tab. You can click this to display a window allowing you to select a different profile name. The activation profile corresponding to the CPC or image of the Details window is effective when the **Activate** task is performed on the object.

Alternately, you can lock or unlock an object for disruptive tasks by right-clicking the object and then click **Toggle lock**. This locks the object if it is unlocked or unlocks the object if it is locked. (Refer to “Performing a task on an object” for information about clicking the second set of menu items.)

Performing a task on an object

You can perform tasks on any object or group of objects in the *Work* area. This is done using *direct manipulation*.

There are several ways to perform direct manipulation. One way is to open an object's menu by right-clicking on the object. The previous section explained the **CPC Details** and **Toggle lock** menu entries. Clicking any of the other entries in the menu displays the next level of the menu as shown in Figure 37 on page 53.

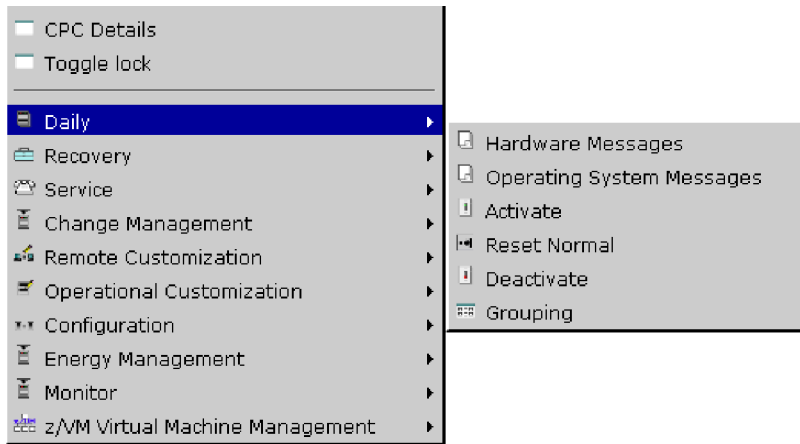


Figure 37. Direct Manipulation

You can click an item on the second menu level to perform that task for the object.

For a single object, you can drag the object with the left mouse button to the appropriate Tasks icon and drop it. Or, you can drag the Tasks icon to the object and drop it.

If you try to use an object that is not valid for a particular task (for example, if the object is the wrong type of object for a task or if the object is busy and the task cannot handle busy objects), the Hardware Management Console presents you with a message window as shown in Figure 38.

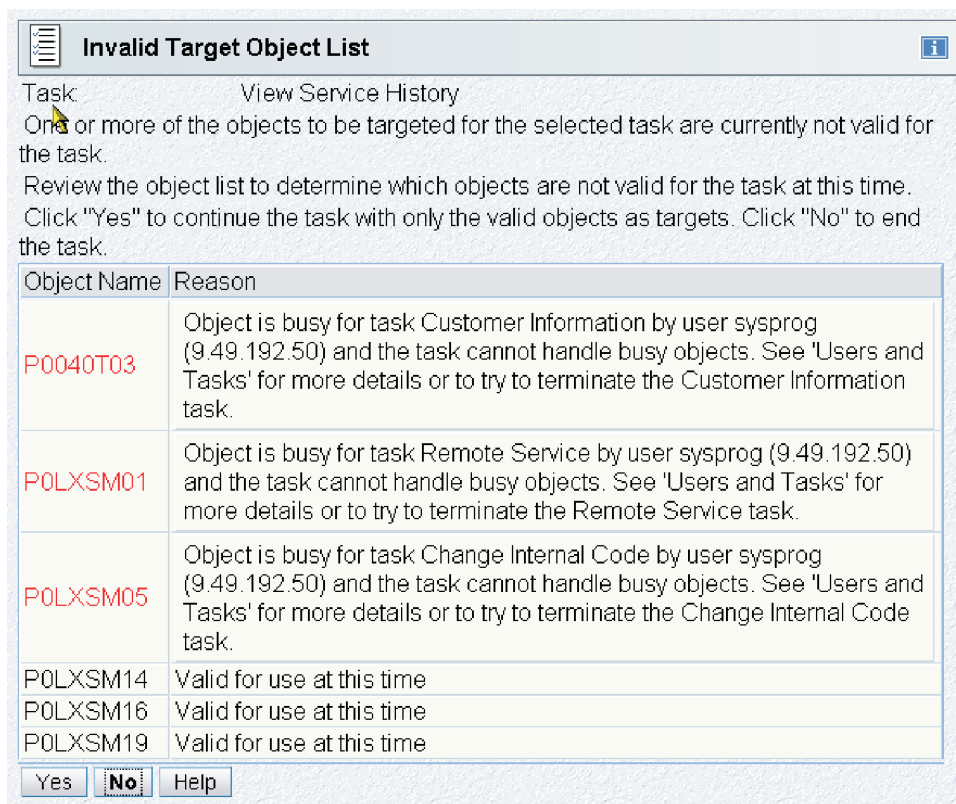


Figure 38. Message window for invalid target objects

For multiple objects, select all the objects you want to perform the task on. Then drag the group by placing the mouse pointer on any one of the selected object's icon, and dragging and dropping the object icon on the task's icon. Or, you can drag the task's icon to any one of the selected objects and drop it. You can also right-click on any one of the objects selected, then select a task to be performed on all the selected objects.

Object locking for disruptive tasks

You can tell when a CPC or CPC image is locked because a locked CPC or image icon has a small yellow lock in the bottom left corner.



The setting of a CPC or CPC image's toggle lock determines whether you can perform a disruptive task on the CPC or CPC image. If you try to perform a disruptive task on a locked object, a window is displayed indicating the object is locked. You can lock an individual object or automatically lock all objects.

To individually lock a CPC or CPC image:

1. Locate the object you want to lock in the *Work* area.
2. Right-click on the object's icon to open its menu.
3. On the menu that is displayed, click **CPC Details** (or **Image Details**).
4. The CPC Details (or Image Details) window is displayed. You can select **Yes** or **No** for **Lock out disruptive tasks**.

An alternate way to lock (or unlock) an individual CPC or CPC image is to:

1. Locate the object you want to lock in the *Work* area.
2. Right-click on the object's icon to open its menu.
3. On the menu that is displayed, click **Toggle Lock**. This locks an object that is unlocked or unlocks an object that is locked.

To lock or unlock all the objects in the *Work* area:

1. Right-click on a spot on the *Work* area without an icon. This displays the menu for the *Work* area as shown in Figure 33 on page 49.
2. Click **Lock all** to lock all the objects in the *Work* area, click **Unlock all** to unlock all the objects in the *Work* area.

There is also an automatic way to lock all the CPCs and CPC images 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*.

1. Open **Console Actions** from the **Views** area.
2. Open **Hardware Management Console Settings** from the **Console Actions Work Area**.
3. Open **Object Locking Settings** from the **Hardware Management Console Settings** work area. The Locking window opens.
4. Select **Automatically lock all managed objects** or **Relock after a task has been run** or both.

If you want to unlock an object or a group of objects, you still need to follow the previously described unlocking procedure.

Note: Because there are really many main user interfaces (one for each logged on user), the Hardware Management Console provides object locking capabilities for each user. This means that users have their own individual object locking settings, managed by using the **Object Locking Settings** task, and their own state information for locked objects. In other words, if you lock or unlock an object, it is not locked or unlocked respectively for other logged-on users.

Monitoring your hardware

The Hardware Management Console continuously monitors the status of its objects and compares them to the object's acceptable status settings.

Note: In this section, the descriptions of the use of color is based on a set of default colors that are set up for you initially. You may override the defaults and associate different colors, or use gray patterns instead of color, by using the **User Settings** task. (For more information, refer to “User Settings” on page 126.)

Acceptable status

Good or acceptable status for all CPCs and CPC images in the processor cluster is indicated by a green background in the *Views* area of the Hardware Management Console workplace window, and by the absence of a red background around the Exceptions icon. Status changes from acceptable to unacceptable, referred to as *Exceptions*, are indicated on the Hardware Management Console workplace window by a color change from green to red. By default, green indicates good, or acceptable status. Red indicates an exception, or that an object has an unacceptable status.

To set the acceptable status for a CPC or CPC image, double click on the CPC or CPC image icon to display the Details window. From the **Acceptable Status** tab you can select the acceptable status settings. The default acceptable status value is *Operating*.

Messages that may require operator attention are indicated by the blue flashing Hardware Messages icon or by the cyan flashing Operating System Messages icon in the *Tasks* area. In addition, to indicate which objects have hardware or operating system messages that require operator attention, the CPC or CPC image icon's background color and its group icon background color will also be blue or cyan.

Unacceptable status

Since the default acceptable status value is *Operating*, all other status values are considered unacceptable. To change the status you select them on the Details window by double-clicking on a CPC or image icon. If an object's status changes to any of the unacceptable values, it is treated as an *Exception* situation. An exception situation is visually indicated by a change of the entire *Views* area background color from green to red as shown in Figure 39. A background color is also displayed for the CPCs or images that have an unacceptable status, and for any of the groups that contain those CPCs or images. The background color depends on what you have selected on the Details window.



Figure 39. Unacceptable status

If an exception situation exists, you can open the **Exceptions** group from the *Views* area to see a subset of only those CPCs or images involved in an exception condition. After you display the Exceptions view, the background of the entire *Views* area changes back to green, and a red background only remains around the Exception icon, the object icon, and the group icon with the unacceptable status as shown in Figure 40.

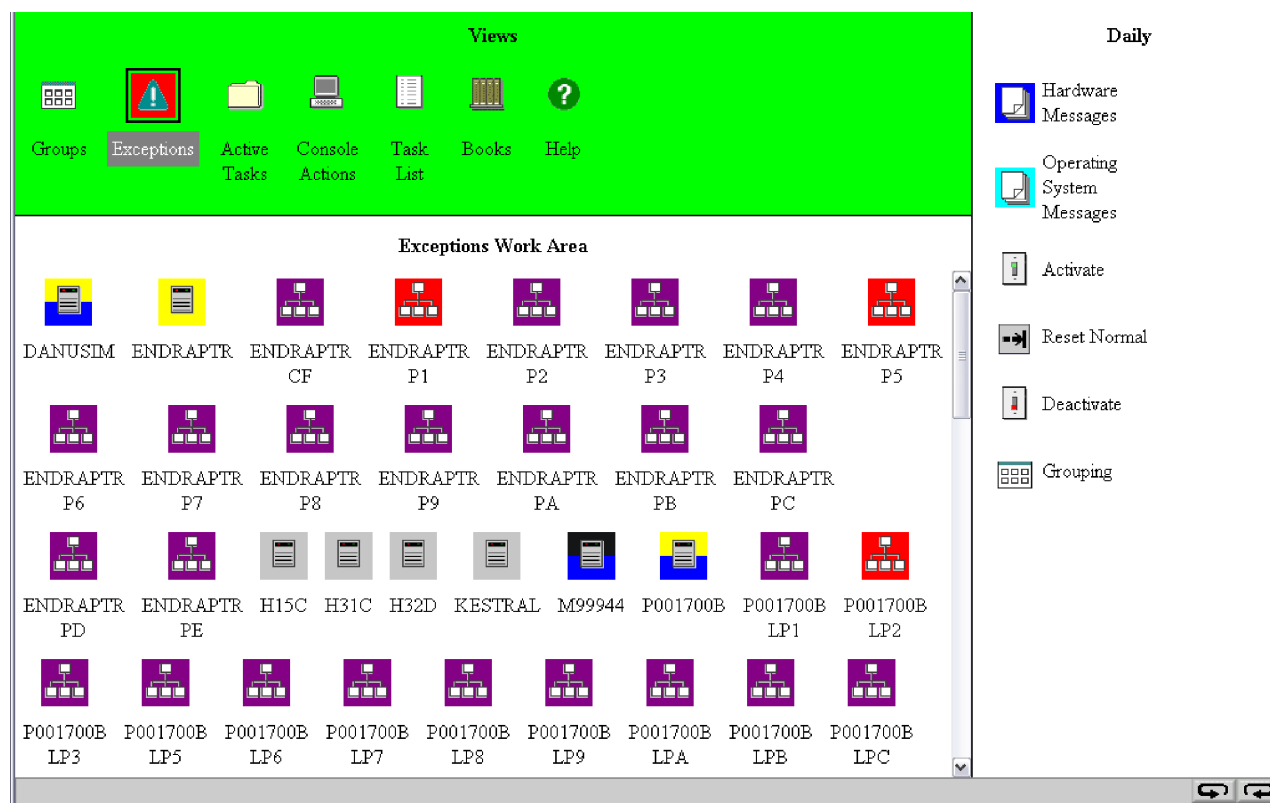


Figure 40. Exceptions work area

This will allow any additional exception situations to be recognized by a color change of the *Views* area. An exception state will remain until the CPC or image returns to a status that you have indicated as acceptable.

Views and work area

Views of your system's objects are represented in the *Views* area (in the upper left portion of the window). Each view provides a different way of looking at information related to your system. After you open the Views objects, they are displayed in the *Groups Work Area* (in the lower left portion of the window) and their contents are available for further action as shown in Figure 32 on page 47.

The following are represented in the *Views* area:

- Groups
- Exceptions
- Active Tasks
- Console Actions
- Task List
- Books
- Help

The *Groups Work Area* displays the objects of your system based on the View that you select. Objects must be displayed in the *Groups Work Area* before you can perform tasks on them.

You can display a particular View by using any of the following methods:

- Double-clicking on the icon in the *Views* area that you want
- Selecting the icon in the *Views* area by clicking on it, then pressing **Enter**.

You can also display two of the choices by opening the pop-up menu. The pop-up menu is a shortcut for navigating the workplace.

1. To open the pop-up menu, click the right mouse button once on any empty area in the *Groups Work Area*. This displays a pop-up menu listing (as shown in Figure 41):

- Groups
- Exceptions
- Active Tasks
- Console Actions
- Task List
- Books
- Style Settings

An arrow to the right of a menu choice indicates additional choices are available on a *cascaded menu*. A cascaded menu provides additional menu choices and may include additional cascaded menus. Each cascaded menu provides a more direct shortcut for locating and opening icons in a particular view.

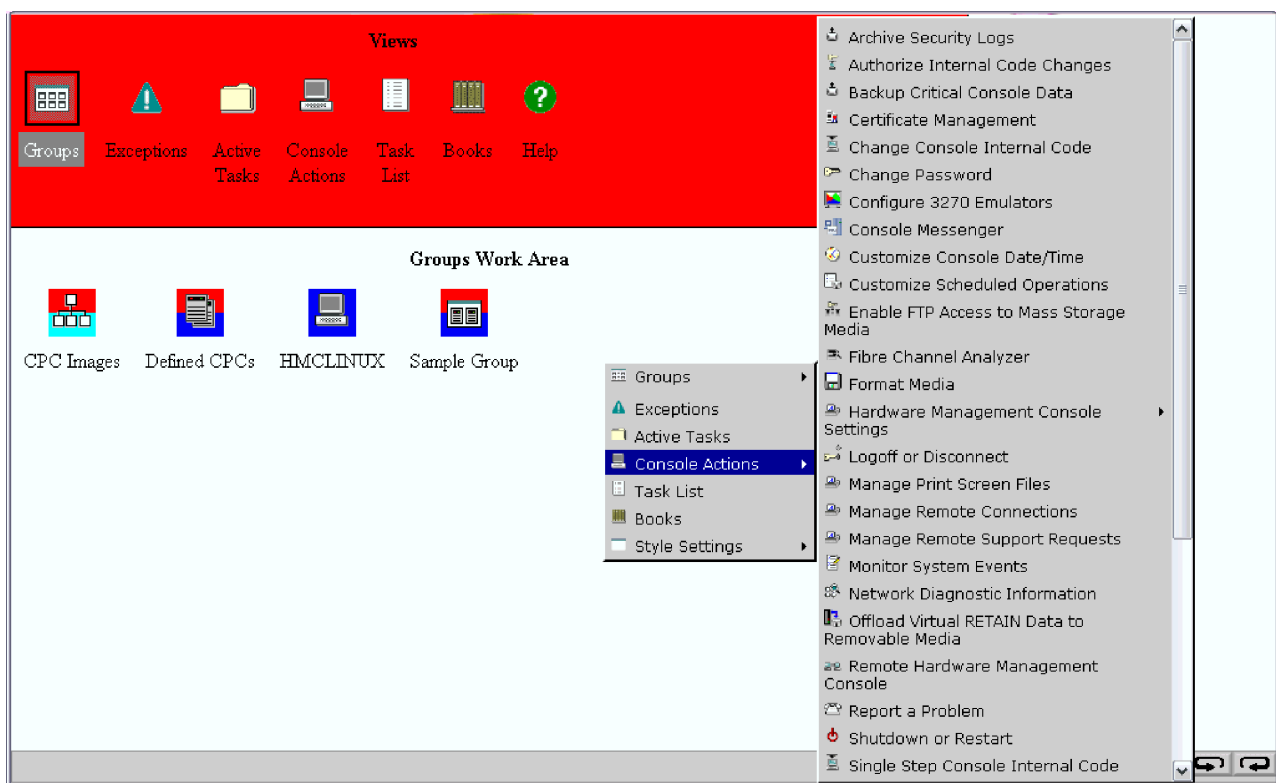


Figure 41. Workplace pop-up menu

2. If you point to either **Console Actions**, **Groups**, or **Style Settings** more choices are displayed for each. Under **Console Actions**, the entire list of console actions is displayed: **View Console Events**, **View Service History**, and so forth. Under **Groups**, your choices include groups of objects, such as **Defined CPCs** and **CPC Images**. Under **Style Settings** a list of options are available that allow you to change the layout of the console actions and *Tasks* area, see the **User Settings** task.

Note: The listings that appear are based off the assigned task roles and managed resource roles your access administrator defined for you. See the **Customize User Controls** and **User Profiles** tasks for more information.

3. Click the item of your choice from the menu.

Groups



The Groups view is displayed initially when you log on to the Hardware Management Console and is the view that you will use most often to run and monitor your system. **Groups** are comprised of logical collections of objects. They provide a quick and easy means for performing tasks against the same set of objects more than once without having to select each object every time the task is run. In addition, status is reported on a group basis, allowing you to monitor your system in a way that you prefer.

Initially, the objects that appear in the *Groups Work Area* are specified by the managed resource roles that were defined for your user ID by your Access Administrator as shown in Figure 42.

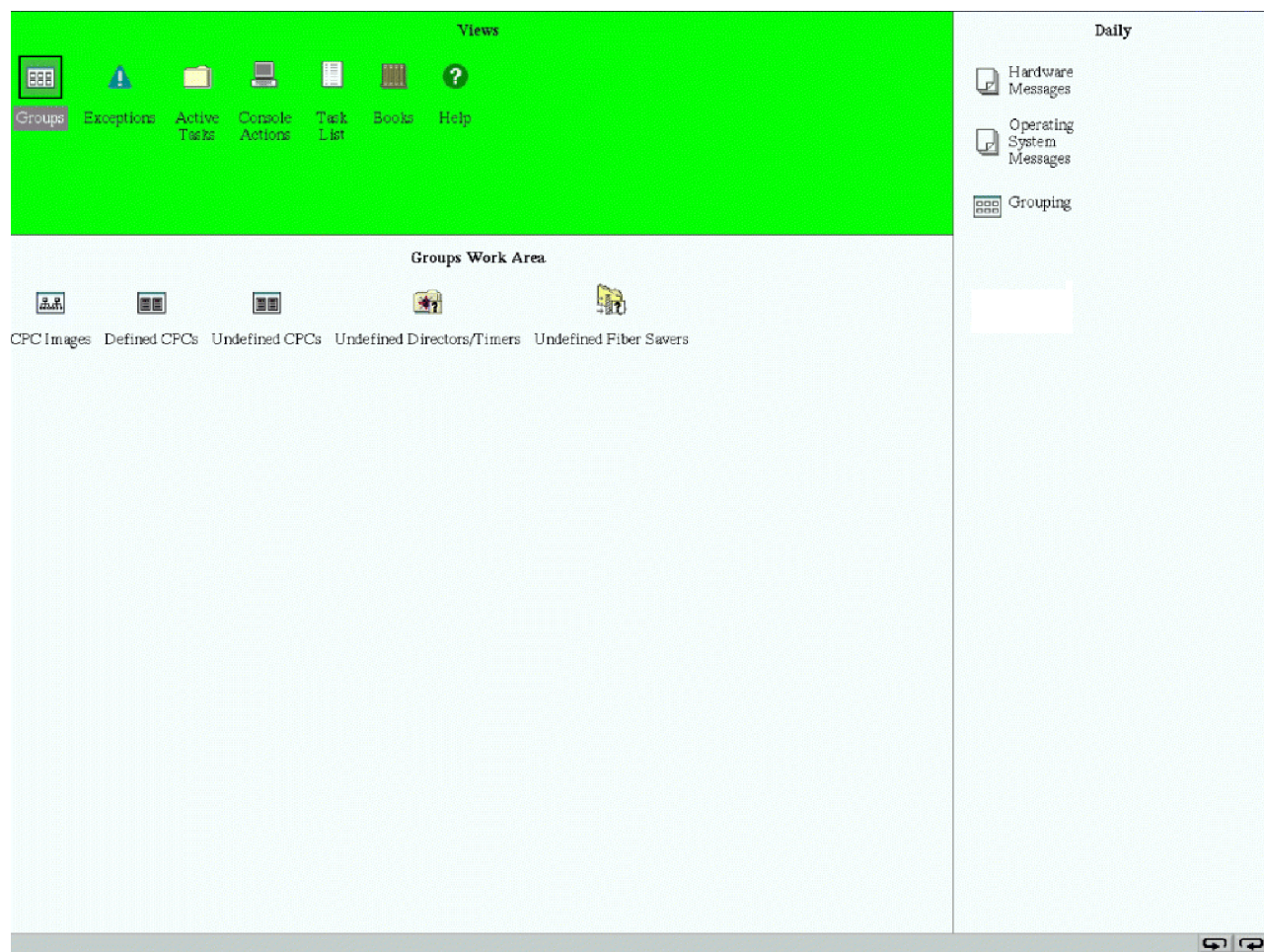


Figure 42. Classic groups work area

You may display the Groups view again by double-clicking with the left mouse button on the Groups icon in the *Views* area. Object icons representing all the system-defined and user-defined groups are displayed in the *Groups Work Area*.

You can select one of the group icons and perform tasks on the objects in a group by dragging it to a task icon, or by dragging a task icon to one of the group icons. You can also nest groups (a group contained within a group).

A **Hardware Management Console** icon can also be displayed in the *Groups Work Area*. This icon represents the Hardware Management Console that you are working on and is displayed only when it is needed. If this icon is displayed, hardware messages have been logged for the Hardware Management Console (see “Hardware messages” on page 77 for more information).

An **Optical Network and System I/O** icon can also be displayed in the *Groups Work Area*. This icon represents the fiber optic connections or system I/O devices of your processor cluster and is displayed only when it is needed. If this icon is displayed, hardware messages have been logged for the optical network or for any system I/O device reported from a Support Element configured to this Hardware Management Console (see “Hardware messages” on page 77 for more information).

An **Fibre Channel Network** icon can also be displayed in the *Groups Work Area*. This icon represents the fibre channel connections of your processor cluster and is displayed only when it is needed. If this icon is displayed, hardware messages have been logged for the fibre channel network reported from a Support Element configured to this Hardware Management Console (see “Hardware messages” on page 77 for more information).

Seven system-defined groups: *CPC Images*, *Defined CPCs*, *Defined Director/Timer Consoles*, *Defined Fiber Savers*, *Undefined CPCs*, *Undefined Director/Timer Consoles*, and *Undefined Fiber Savers* are provided with your system. These groups consist of all images, CPCs, ESCON Director and Sysplex Timer consoles, and 2029 Fiber Savers that make up your processor cluster. It is from these seven system-defined groups that you will create other user-defined groups as you want to work with them.

The following are represented in the *Groups Work Area*:

- CPC images
- Defined CPCs
- Defined directors/timers
- Defined fiber savers
- Undefined CPCs
- Undefined director/timer consoles
- Undefined fiber savers
- User-defined groups
- Hardware Management Console
- Optical network and system I/O
- Fibre channel network
- z/VM Virtual Machine Management (is displayed if one or more CPC images are running z/VM V5.3 or later and at least one z/VM virtual machine has been selected to manage)

CPC images

An image is either of the following:

- In LPAR mode, a partition where a coupling facility control code (CFCC) or an operating system can be run.
- In non-LPAR mode, the system itself where an operating system can be run.

Note: CPC images will not be displayed if Service Status is enabled for the CPC. For information about Service Status, see “Service Status” on page 155.

The **CPC Images** group displays all images in the processor cluster as shown in Figure 43 on page 61.

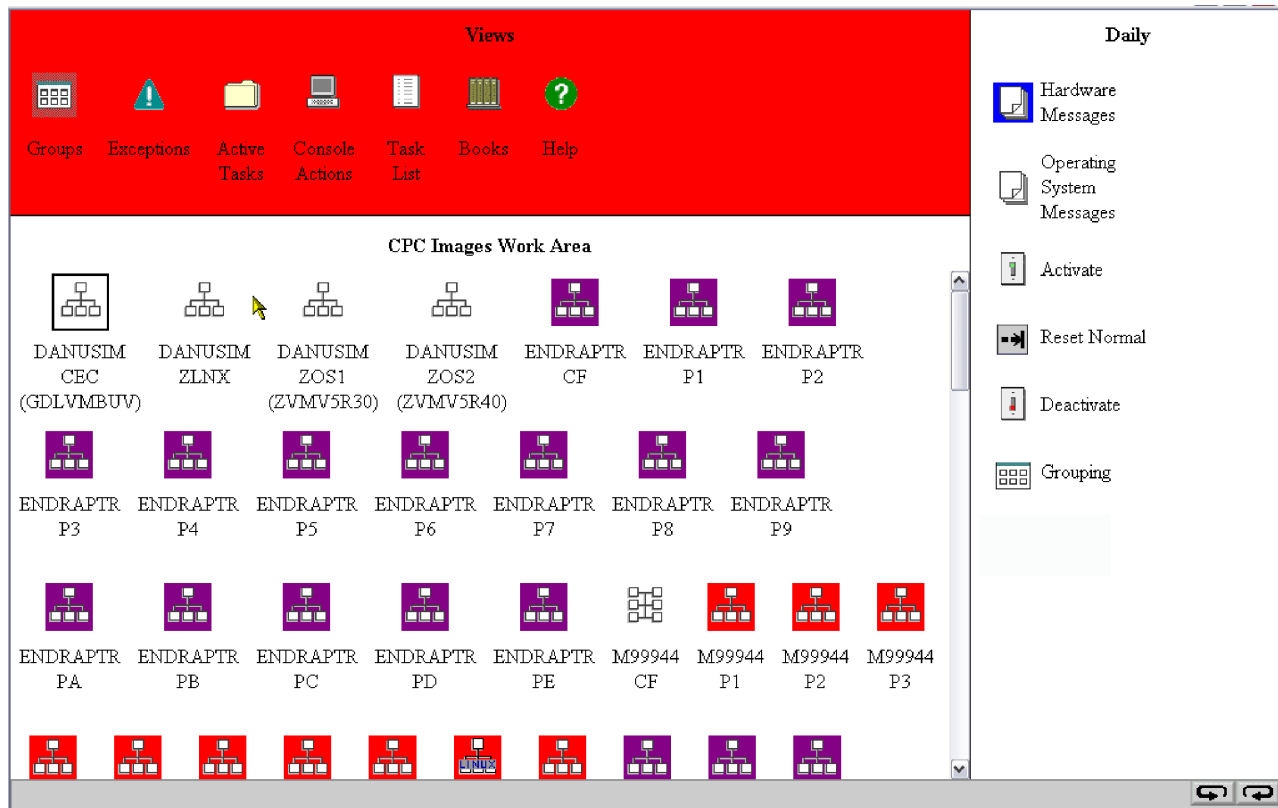


Figure 43. CPC images group window

Defined CPCs

Note: If you cannot access defined CPCs, contact your access administrator.

Defined CPCs display all of the CPCs that have been defined to your Hardware Management Console as shown in Figure 44 on page 62. Tasks cannot be performed on a CPC until it is defined. If a CPC is not defined, it will be a part of the **Undefined CPCs** when it is powered on. To define the CPC, see the **Add Object Definition** task (see “Add Object Definition” on page 181 for more information).

After a CPC is defined, it is removed from the Undefined CPCs group and added to the Defined CPCs group. From the Defined CPCs group, the CPC can be grouped into one or more user-defined groups. A defined CPC will remain as a part of the Defined CPCs group until its definition is removed, regardless of its power state.

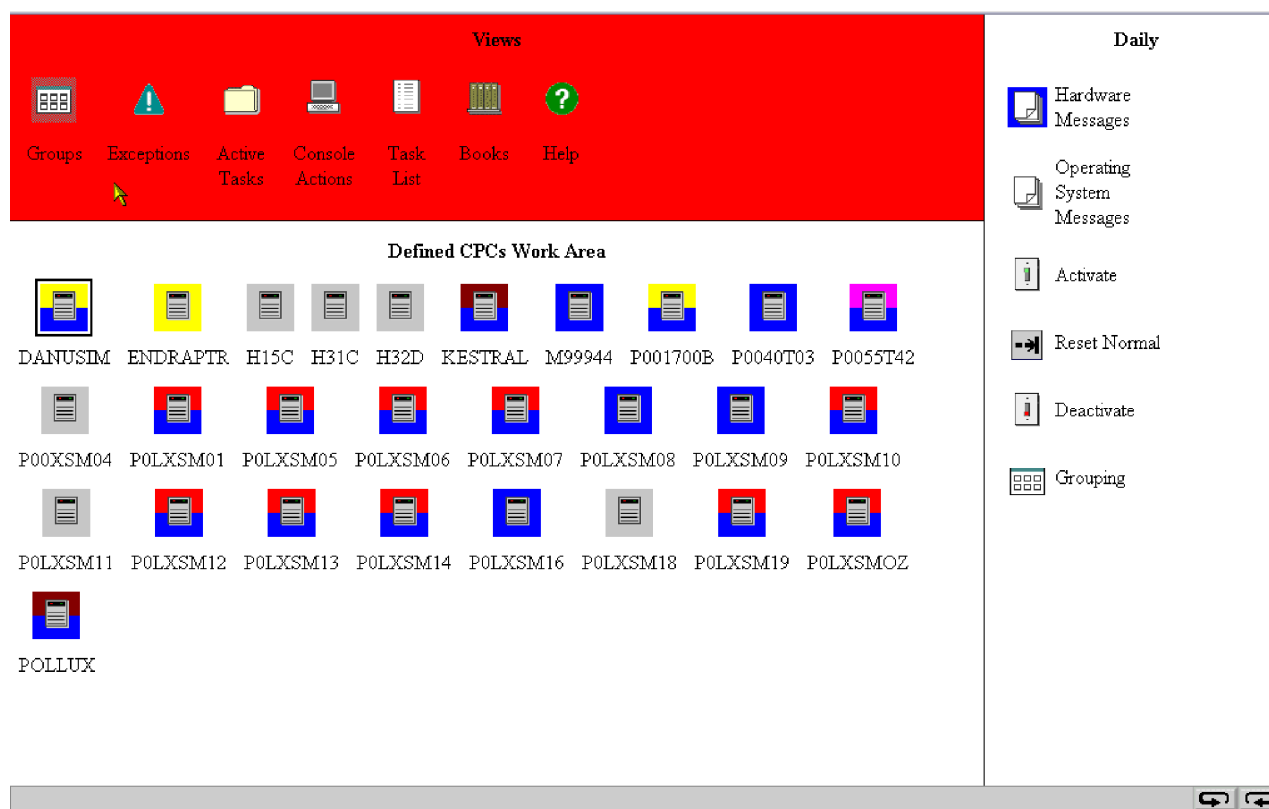


Figure 44. Defined CPCs group window

There are two types of status messages that can affect the CPC icon in the *Defined CPCs* work area:

- Degraded
- Service Required.

Degraded:

This displays under the CPC icon name and indicates that although the system is still operating, one or more of the following conditions exist:

- Loss of channels due to CPC hardware failure
- Loss of memory
- One or more books are no longer functioning
- The ring connecting the books is open
- Capacity Backup (CBU) resources have expired
- Processor frequency reduced due to temperature problem
- CPC was IMLed during temperature problem.

To view what conditions caused this message to display on a CPC:

1. Double-click on the desired CPC icon. The Details window for the selected CPC opens.
2. Click **Degrade reasons....** The Degraded Details window displays the current list of reasons why the selected CPC is degraded.

Service required:

This displays in the *Status* box on the Details window of the CPC. Your CPC is shipped with redundant hardware; that is, you have more than the required number of hardware parts to operate the CPC. When a part fails causing the use of the last redundant part of that type, you now have just the required number of parts to keep the CPC running. By displaying this message, it is a reminder to both you and

your service representative that repairs should be made at the earliest possible time before additional parts fail that would now make your CPC non-operating. Some of the conditions that will cause this message to display on the Details window are:

- Loss of a Bulk Power Assembly (BPA)
- Loss of communications to the alternate Support Element
- No more spare Processing Units (PUs)
- Not enough spare PUs to support either Capacity BackUp (CBU) or Disaster Recovery Assurance (if either feature is installed)
- Memory sparing threshold reached
- Multiple Chip Module (MCM) is defective
- Oscillator card is defective
- ETR card is defective
- FSP/STP card is defective
- The Service Network is in N-mode.

Defined directors/timers

This system-defined group contains all Director/Timer consoles defined to the Hardware Management Console whether they were automatically discovered or defined using the Undefined Director/Timer Definition Template. This group will not appear in the *Groups Work Area* until you have defined a Director/Timer console. For more information on defining director/timer consoles to the Hardware Management Console, see “Undefined director/timer consoles” on page 65.

A **Director/Timer console** is an object that represents either:

- An ESCON Director console
- A Sysplex Timer console.

Defined Director/Timer consoles are objects that have been customized to enable operating the consoles from the Hardware Management Console and are the targets of the following Hardware Management Console tasks:

- *Single Object Operations*. Use this task to operate a defined Director/Timer console from the Hardware Management Console through a web browser. See “Single Object Operations” on page 149 for more information.
- *Grouping*. Use this task to create, change, or delete user-defined groups of defined Director/Timer consoles. See “Grouping” on page 139 for more information.
- *Object Definition tasks*. Use these tasks to change or remove the object definitions of defined Director/Timer consoles. See “Object Definition” on page 181 for more information.

Defined fiber savers

This group contains all 2029 Fiber Savers defined to the Hardware Management Console using the Fiber Saver Definition Template. This group will not appear in the Groups Work Area until you have defined a Fiber Saver object. For more information on defining 2029 Fiber Savers to the Hardware Management Console, see “Undefined fiber savers” on page 65.

Defined Fiber Savers are objects that have been customized to enable call-home support from the Hardware Management Console to the IBM Service Support System (RETAIN). Because the Hardware Management Console does not have access to the 2029 FRU information, all calls are reported as type 2. The following information about the error is provided:

- Time of failure
- Error identification code
- Description of the error
- Shelf ID
- Shelf slot.

After the IBM Service Support System receives the data, they can contact the customer to further isolate the problem before sending a service representative.

For more information on the 2029 Fiber Saver, and especially on *Shelf Description naming information*, see *2029 Fiber Saver Maintenance*, SC28-6807 or *2029 Fiber Saver Planning and Operations Guide*, SC28-6808.

Undefined CPCs

Note: If you cannot access undefined CPCs, contact your access administrator.

The Undefined CPCs group displays all of the CPCs in the processor cluster that:

- Are physically installed
- Have their Support Element powered on
- Have the same Domain Name as the Hardware Management Console
- Have not been defined to your Hardware Management Console.

A CPC in this group must be defined before tasks can be performed on it. Status is not reported for objects in the Undefined CPCs group. To define CPCs, use “Add Object Definition” on page 181.

In addition to Undefined CPCs, this group also contains the **CPC Manual Definition** icon.

CPC Manual Definition:

Local Hardware Management Consoles can automatically detect the presence of Support Elements and automatically set up all the necessary internal configuration information for communication without additional information from the users. For remote Hardware Management Consoles, users must provide additional addressing information to perform this configuration.

Use **CPC Manual Definition** to define a CPC when TCP/IP connectivity exists between the Hardware Management Console and the CPC:

1. Open the **Task List** from the **Views** area.
2. Open **Object Definition** from the **Task List Work Area**.
3. Open **Groups** from the **Views** area.
4. Open **Undefined CPCs** group.
5. Select **CPC Manual Definition**.
6. Drag and drop **CPC Manual Definition** on **Add Object Definition** in the **Object Definition** tasks area. The Manual Add Object Definition window opens.
7. Specify the TCP/IP address in the **Addressing Information** field and click **OK**. The Hardware Management Console tries to contact the Support Element and exchange the remaining information necessary to complete the configuration process.

Note: The Manual Add Object Definition window remains open with the last entered TCP/IP address until you have added the appropriate CPCs. When you have completed this task, click **Cancel**.

You can connect a remote Hardware Management Console to a Support Element using TCP/IP through bridges or routers.

- Using **TCP/IP bridges** to interconnect the Support Element's local LAN to the company's network requires that the Support Element be a part of a TCP/IP subnet that is the same as the subnet to which the Support Element is bridged. Therefore, information that must be configured in a remote Hardware Management Console is the TCP/IP address of the target Support Element.

The bridge filters must be configured to allow TCP/IP flows to cross the bridge. The bridges must be configured and operational before Support Elements can be manually defined in the remote Hardware Management Console.

Note: For ethernet LANs, there are two different types of ethernet formats: Ethernet Version 2 and 802.3. All devices on the ethernet LAN must use the same format. All Hardware Management Consoles and Support Elements use the Ethernet Version 2 format. If you need to use 802.3 format, contact the IBM Service Support System for assistance.

- Using a **TCP/IP router** to interconnect the Support Element's local LAN to a company's network requires that the Support Element be on a unique subnet and that the routers in the network know how to deliver packets to that subnet. Therefore, information that is necessary to configure a remote Hardware Management Console to a Support Element through a TCP/IP network is the TCP/IP address of the Support Element. The routers must be configured and operational before the remote Hardware Management Console can be configured to connect to the Support Element.

If Routing Information Protocol (RIP) packets do not flow from the router to the Hardware Management Console, then the default route will also need to be defined using the **Customize Network Settings** task.

For information about using CPC Manual Definition as the target object for performing the **Add Object Definition** task, see "Add Object Definition" on page 181.

Undefined director/timer consoles

Note: If you cannot access undefined director/timer/consoles, contact your access administrator.

This system-defined group contains Director/Timer consoles, if any, that can be defined to the Hardware Management Console but currently are not defined to it. The group also contains a template for manually identifying and defining Director/Timer consoles that the Hardware Management Console cannot automatically discover.

A *Director/Timer console* is an object that represents either:

- An ESCON Director console
- A Sysplex Timer console.

Undefined Director/Timer consoles and the Director/Timer Console Manual Definition Template can be targets of the **Add Object Definition** task only. To define Director/Timer consoles, use the **Add Object Definition** task.

To locate the Director/Timer Definition Template and define a director/timer:

1. Open **Groups** in the **Views** area.
2. Open **Undefined Director/Timer** in the **Groups Views Area**. The **Director/Timer Definition Template** is displayed in the **Undefined Director/Timer Work Area**.
3. Drag and drop the template on **Add Object Definition** task in the **Object Definition** tasks area. The Director/Timer Console Manual Add Object Definition window is displayed.
4. Enter the **TCP/IP address** in the input field.
5. Click **Find**.
6. If you get the message that the director/timer was contacted, click **Save** to add the Director/Timer.
7. After the director/timer is added, click **OK** in the Task Completed Successfully window. The director/timer is now added to the **Defined Director/Timer** group.

Undefined fiber savers

Note: If you cannot access undefined fiber savers, contact your access administrator.

This system-defined group contains a template for manually identifying and defining 2029 Fiber Savers. Undefined fiber savers and the Fiber Saver Manual Definition Template can be targets of the **Add Object Definition** task only.

To locate the Fiber Saver Manual Definition Template and define a fiber saver:

1. Open the **Task List** from the **Views** area.
2. Open **Object Definition** from the **Task List Work Area**.
3. Open **Groups** from the **Views** area.
4. Open the **Undefined Fiber Savers** group.
5. Click **Fiber Saver Manual Definition Template**.
6. Drag and drop the template on **Add Object Definition** in the **Object Definition** tasks area. The IBM Fiber Saver (2029) Manual Add Object Definition window opens.
7. Enter the **TCP/IP address** and the **Community name** in the input field.
8. Click **Find**.
9. If you get the message that the Fiber Saver was contacted, click **Save** to add the Fiber Saver.
10. After the Fiber Saver is added, click **OK** in the Task Completed Successfully window. The Fiber Saver is now added to the **Defined Fiber Savers** group.

User-defined groups

There may be one or more user-defined groups already defined on your Hardware Management Console. You can create others, delete the ones that were created, add to created groups, or delete from created groups by using the **Grouping** task.

Note: The system-defined groups (Defined CPCs, CPC Images, and Undefined CPCs) cannot be deleted.

To use the **Grouping** task:

1. Open the **Task List** from the **Views** area.
2. Open **Daily** from the **Task List Work Area**.
3. Open **Groups** from the **Views** area.
4. Open the group that contains the CPCs or images that you want to group.
5. Select one or more objects.
6. Drag and drop the selected objects on **Grouping** in the **Daily** tasks area.
7. The Manage Groups window opens allowing you to add the selected object(s) to an existing group, remove the selected object(s) from a group, create a new group, remove the group, create a new pattern match group, or edit an existing pattern match group. Online help is available to guide you through completion of this task. For more information about grouping, see "Grouping" on page 139.

Hardware Management Console

The Hardware Management Console icon represents the Hardware Management Console that you are using. It only displays in the *Groups Work Area* when Hardware Messages have been logged for the Hardware Management Console. Messages logged for the Hardware Management Console are messages about the Hardware Management Console and ethernet and token-ring network activity that provide the links to the CPC Support Elements.

To view these messages, drag the Hardware Management Console icon to any tasks area and drop it on the Hardware Messages icon.

For more information about Hardware Messages, see "Hardware messages" on page 77.

Optical network and system I/O

The Optical Network and System I/O icon represents messages resulting from the Problem Analysis Focal Point function analysis of errors from either fiber optic connections or system I/O devices.

Fiber optic connections are used by CPCs to communicate with Input/Output (I/O) devices or a coupling facility. Those connections are:

- ESCON - optical I/O connections
- FICON - optical I/O connections
- FCP - optical I/O connections
- Coupling Facility Channels - optical coupling facility links
- InterSystem Coupling links - optical coupling connections between zSeries servers.

Optical errors are problems that may affect more than one CPC and, therefore, need to be analyzed at a common point (a Problem Analysis Focal Point).

Some system I/O devices, mostly tape and DASD products, report errors to their operating system. If Optical Error Analysis is **Enabled** on the Hardware Management Console, each configured Support Element will forward reported I/O errors to the Problem Analysis Focal Point where they will be analyzed and possibly reported to the service provider. To enable Optical Error Analysis, see the **Customize Console Services** task.

To ensure that duplicate problem reporting does not occur, only one Hardware Management Console (of all the Hardware Management Consoles configured to control a Support Element) should have Optical Error Analysis enabled.

To view the messages related to Optical Network and System I/O, drag the icon to any tasks area and drop it on the Hardware Messages icon. For more information about Hardware Messages, see “Hardware messages” on page 77.

Fibre channel network

The Fibre Channel Network icon represents messages resulting from the Problem Analysis Focal Point function analysis of errors from fibre channel devices.

Fibre channel connections are used by CPCs to communicate with FICON connections.

Fibre channel errors are problems that may affect more than one CPC and, therefore, need to be analyzed at a common point (a Problem Analysis Focal Point).

If Fibre Channel Analysis is **Enabled** on the Hardware Management Console, each configured Support Element will forward reported fibre channel errors to the Problem Analysis Focal Point where they will be analyzed and possibly reported to the service provider. To enable Fibre Channel Analysis, see the **Customize Console Services** task.

To ensure that duplicate problem reporting does not occur, only one Hardware Management Console (of all the Hardware Management Consoles configured to control a Support Element) should have Fibre Channel Analysis enabled.

To view the messages related to Fibre Channel Network, drag the icon to any tasks area and drop it on the Hardware Messages icon. For more information about Hardware Messages, see “Hardware messages” on page 77.

Managed z/VM virtual machines

The Managed z/VM Virtual Machines icon represents the virtual machines being managed by the Hardware Management Console. This group of objects is created from a CPC image running z/VM V5.3 or later, see “Choose z/VM Virtual Machines to Manage” on page 195 for more information. Double-clicking on this icon displays the **Managed z/VM Virtual Machines Work Area**. You can display the details about each of the virtual machines by double-clicking on the icon or right-clicking with the mouse, then choose **z/VM Virtual Machine Details** as shown in Figure 45 on page 68.

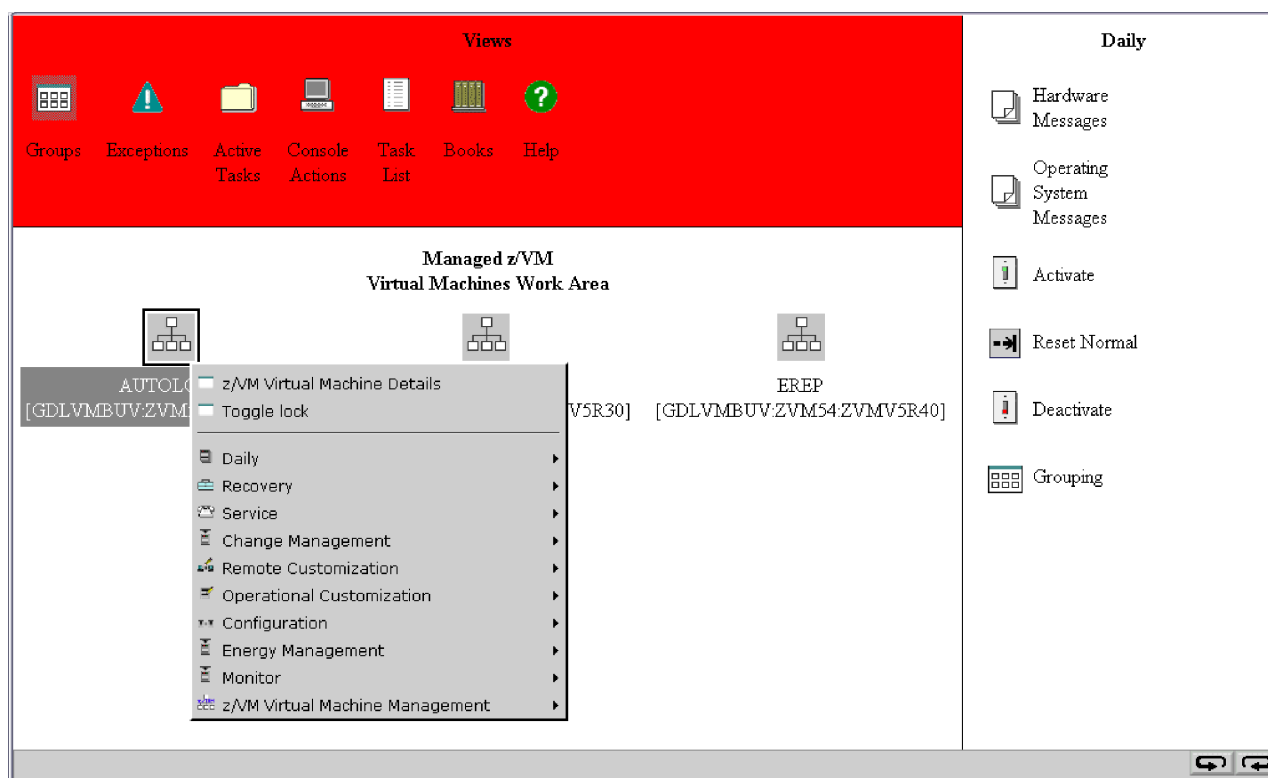


Figure 45. z/VM virtual machines work area

Clicking **z/VM Virtual Machine Details** displays the details about the virtual machine. Figure 46 shows an example of a z/VM Virtual Machine Details window.

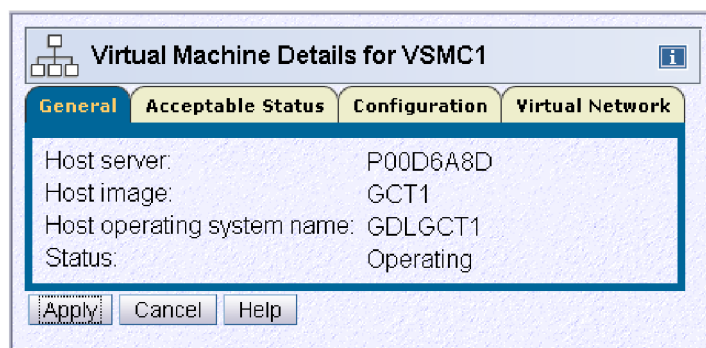


Figure 46. Virtual machine details window

The Virtual Machine Details window includes the following tabs:

General

Specifies the current status of the virtual machine and other information about the virtual machine's operating environment.

Acceptable Status

Displays the settings that determine which virtual machine statuses are acceptable and which statuses are unacceptable. The Hardware Management Console reports when the virtual machine status becomes unacceptable.

Level 01a

Configuration

Specifies more detailed information about the virtual machine. This information is available only when the virtual machine is currently active.

Virtual Network

Specifies information about the virtual network adapters defined for the virtual machine. This information is available only when the virtual machine is currently active and there are virtual network adapters defined for the virtual machine.

Exceptions



Display the Exceptions view by double-clicking with the left mouse button on the Exceptions icon in the **Views** area. Object icons representing all the CPCs and images that are in an exception state, due to an unacceptable status condition, is displayed in the *Exceptions Work Area* as shown in Figure 47. If no CPCs or images are in an exception state, the Exceptions Work Area will be empty.

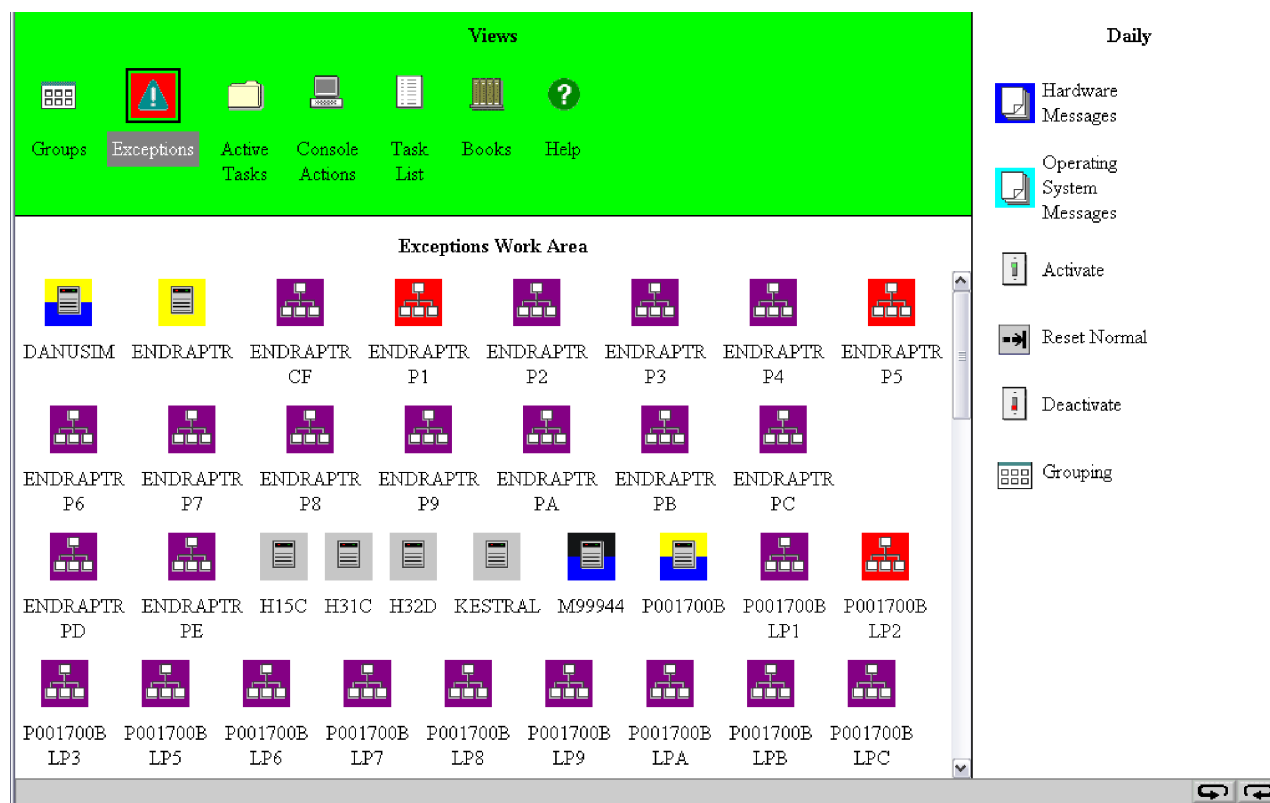


Figure 47. Exceptions work area

You can recognize that an object is in the Exceptions view by one or both of the following visual indicators:

- The entire top Views portion of the Hardware Management Console workplace window has a background color that indicates that an exception has occurred.
- The background of the Exceptions icon has a background color that indicates that an object has exceptions.

To view the current status and the acceptable status values for any of the objects in the *Exceptions Work Area*, double-click on their icons to display the Details window. To initiate a corrective action, select one or more of the CPC or image icons in the *Exceptions Work Area* and perform tasks by dragging them to a task icon, or by dragging a task icon to one of the CPC or image icons.

Note: An object in the *Exceptions Work Area* will display the activation profile that was last used in the “Activation Profile” field. An activation of an object in the *Exceptions Work Area* will attempt to activate the object with the last used profile to return it to its previous status. Under some conditions the

“Activation Profile” field of an object in the *Exceptions Work Area* could have no activation profile associated with it. If activation is needed to resolve an exception condition for an object that has no activation profile associated with it, it is recommended that the object be activated from a user-defined group or that an activation profile be selected from the object's details window.

See “Monitoring your hardware” on page 55 for more information about Exceptions and the use of color.

Active tasks



Display the Active Tasks view by double-clicking with the left mouse button on the Active Tasks icon in the *Views* area. This view is useful when you have minimized the Progress windows for one or more tasks that are in progress simultaneously. Object icons representing all the tasks that are currently in progress, or those tasks that have completed but whose ending status has not been reviewed, is displayed in the *Active Tasks Work Area*.

If there are active icons in the *Active Tasks Work Area*, you can double-click them to display the Progress window again for that task. When a task completes, the Progress window for that particular task is automatically displayed again, allowing you to respond to the final status.

Console actions



Display the Console Actions view by double-clicking with the left mouse button on the Console Actions icon in the *Views* area. Object icons representing all the actions that can be performed on the Hardware Management Console and its internal code are displayed in the *Console Actions Work Area* as shown in Figure 48. These actions are used for setting up the Hardware Management Console, maintaining its internal code, and servicing the Hardware Management Console. Most likely, you will not use these actions on a regular basis.

Note: The layout of the console actions in the work area uses the default sort order for the classic style user interface. You can change the layout from the **User Settings** task on the **Classic Style** tab or select **Style Settings** from the pop-up menu in the work area. Figure 48 displays the console actions sort order by ascending name.

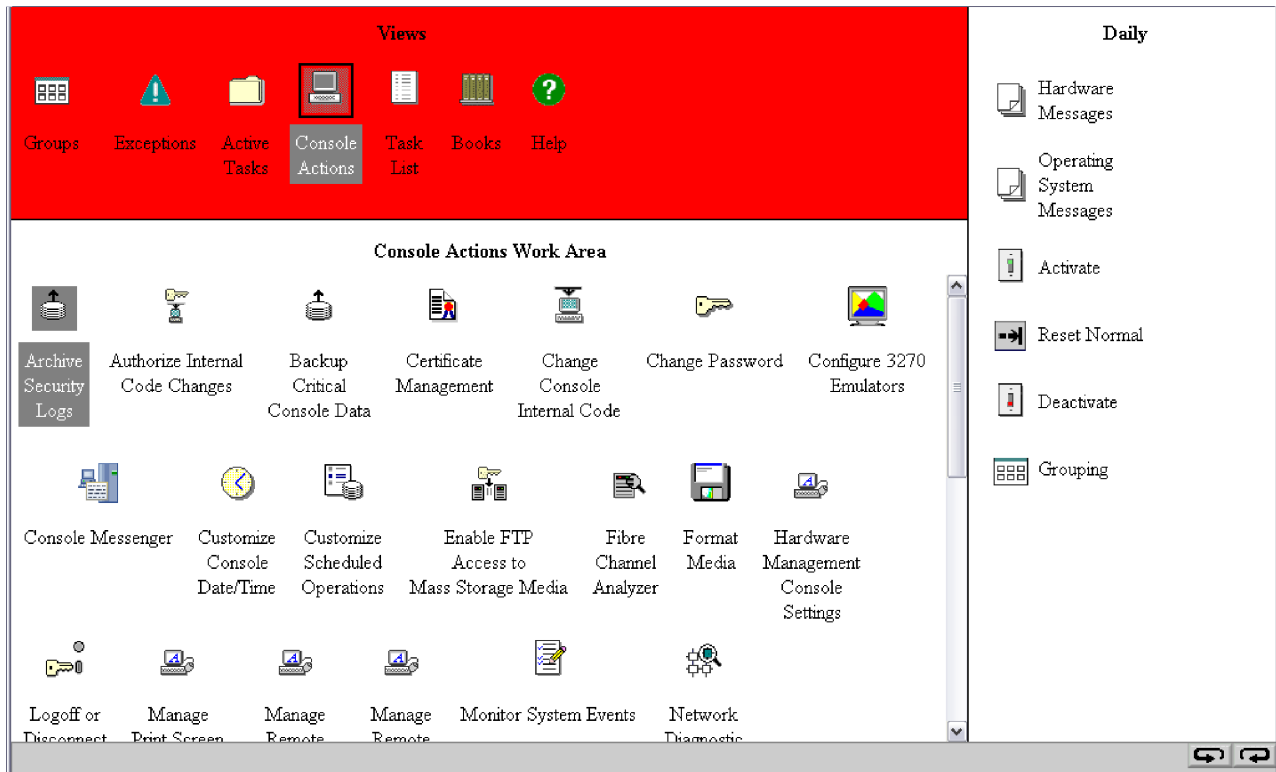


Figure 48. Console actions work area

To begin any console action task while using the classic style user interface:

1. Open **Console Actions** from the **Views** area.
2. Open the task that you want to perform from the **Console Actions Work Area**.
3. The window for that task opens and you can proceed with the functions that need to be performed for that task.

The following tasks, arranged by default sort order, are represented in the *Console Actions Work Area* and are described in further detail alphabetically in Chapter 5, “Hardware Management Console tasks,” on page 81:

- View Console Events
- View Console Service History
- Save/Restore Customizable Console Data
- Customize Console Date/Time
- Change Console Internal Code
- Analyze Console Internal Code
- Single Step Console Internal Code
- Backup Critical Console Data
- Perform a Console Repair Action
- View Console Information
- User Profiles
- Customize User Controls
- Password Profiles
- Manage Users Wizard
- Manage Enterprise Directory Server Definitions
- User Templates
- User Patterns
- User Settings
- Console Default User Settings
- Customize Scheduled Operations
- Transmit Console Service Data
- Authorize Internal Code Changes
- Domain Security
- Installation Complete Report
- Report a Problem
- View Console Tasks Performed
- Network Diagnostic Information
- Rebuild Vital Product Data
- Archive Security Logs
- View Security Logs
- Save Upgrade Data
- Reassign Hardware Management Console
- Enable Electronic Service Agent
- Format Media
- Offload Virtual RETAIN Data to Removable Media
- Copy Console Loges to Media
- Transmit Vital Product Data
- Manage Remote Support Requests
- Manage Remote Connections
- Audit and Log Management
- Block Automatic Licensed Internal Code Change Installation
- Certificate Management
- Change Password
- Console Messenger
- Create Welcome Text
- Configure 3270 Emulators
- Enable FTP Access to Mass Storage Media
- Fibre Channel Analyzer
- Hardware Management Console Settings
- Logoff or Disconnect
- Manage Print Screen Files
- Manage SSH Keys
- Manage Web Services API Logs
- Monitor System Events
- Remote Hardware Management Console
- Restore Legacy HMC Data

Level 01a

- Shutdown or Restart
- Tip of the Day
- Users and Tasks
- View Licenses
- View PMV Records
- What's New

In addition to these tasks, the **Hardware Management Console Settings** task includes the following tasks under it:

- Configure Data Replication
- Customize API Settings
- Customize Auto Answer Settings
- Customize Automatic Logon
- Customize Console Services
- Customize Customer Information
- Customize Modem Settings
- Customize Network Settings
- Customize Outbound Connectivity
- Customize Product Engineering Access
- Customize Remote Service
- Object Locking Settings

Task list



Display the Task List view by double-clicking with the left mouse button on the Task List icon in the *Views* area. The Hardware Management Console is initially displayed with Daily tasks icons displayed in the *Tasks* area on the right portion of the window as shown in Figure 49.

Note: The z/VM Virtual Machine Management icon is displayed in the Task List only when one or more CPC images are running z/VM V5.3 or later.

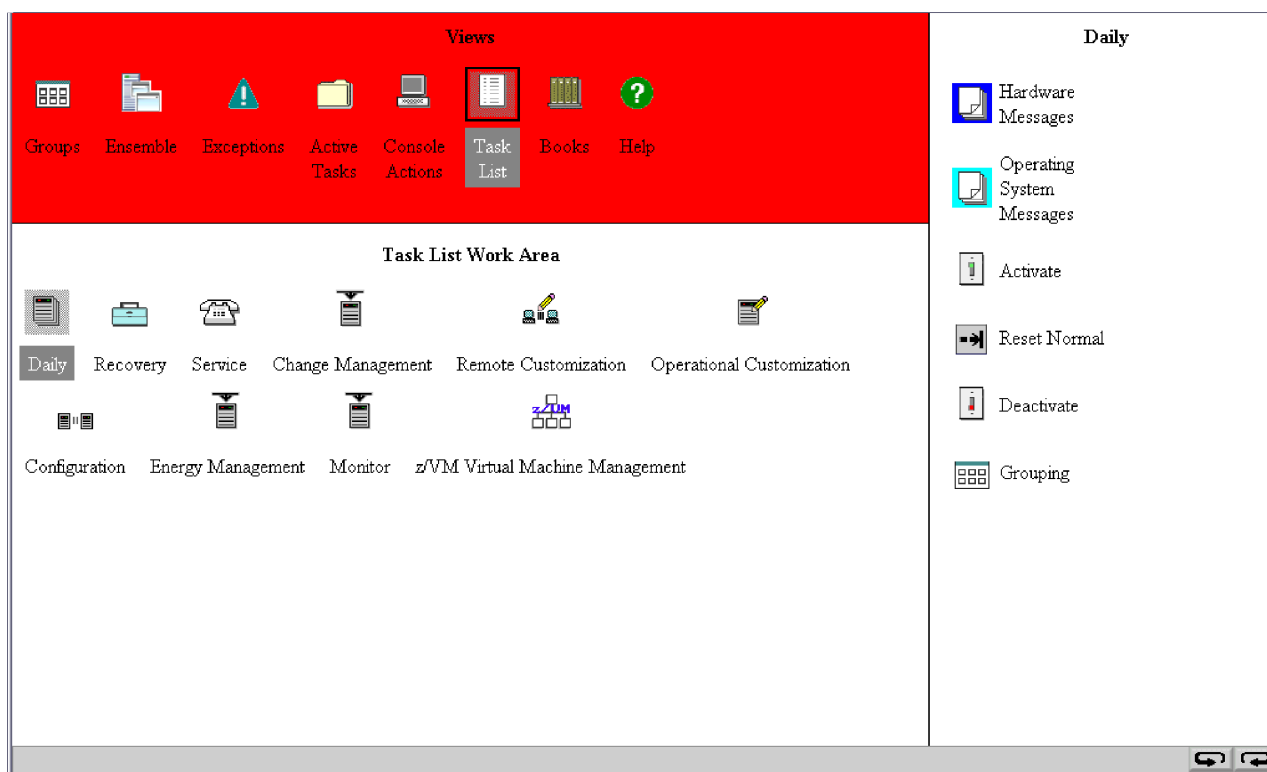


Figure 49. Task list work area

To change to a different set of tasks, you can use any one of the following methods:

- Double-click on one of the icons displayed in the *Task List Work Area*.
- Click on either the Task Ring Forward button or the Task Ring Backward button until the desired tasks are displayed. The Task Ring buttons are on the bottom right corner of the tasks area.

Note: If the Task Ring buttons do not appear, you can click the **Maximize** button that is located in the upper right corner of the window.

- Right-click in the Task List area and then select a different task group from the pop-up menu.

To begin these tasks on an object(s) using the classic style user interface:

1. Open the **Task List** from the **Views** area
2. Open the task list from the **Task List Work Area**.

3. Open **Groups** from the **Views** area.

For individual CPCs:

- a. Open the group that contains the CPCs you want to display.
- b. Select one or more objects.

For a group of CPCs:

- a. Select the group of CPCs that you want to display

4. Drag and drop the selected object on the task you want from the task list you opened.

5. The window for that task is displayed and you can proceed with the functions that need to be performed on the object.

The following are represented in the *Task List Work Area* and described in further detail in Chapter 6, "Server tasks," on page 137:

- Daily
- Recovery
- Service
- Change Management
- Remote Customization
- Operational Customization
- Object Definition
- Configuration
- Energy Management
- Monitor
- z/VM Virtual Machine Management (is displayed if one or more CPC images is running z/VM V5.3. or later)

Each task list contains the following messages common to all task lists:

- Hardware Messages
- Operating System Messages

Hardware messages



Displays consolidated hardware related messages for all selected hardware in the processor cluster, including your Hardware Management Console. These messages are available to all default user IDs.

Note: Depending on your user task role, you may only view the hardware messages.

When a message is logged, the Hardware Messages icon alternates between a light and dark background. The hardware object (CPC or Hardware Management Console) with a message pending is indicated by a dark background on its object icon. By default, the dark background color of the object icon and the Hardware Messages icon is blue.

A message is a brief, one-line description of an event, such as a report of a Hardware Management Console failure. You can view further explanation and any recommended operator action for a single message by selecting one or more messages and then click **Details....** The message details and any recommended operator action display, one at a time, for each selected message.

Hardware messages for all of the hardware objects are stored on the Hardware Management Console hard disk in the Message Log File. Because the Message Log File limits the number of messages to five hundred, try to view, act on, and delete messages promptly. Messages received over this limit will cause

the oldest messages to be lost. Delete selected messages from the list by clicking **Delete**. A window displays for confirmation before any messages are deleted.

Note: Some messages are deleted automatically after you view the message details. These messages generally provide information only, and are deleted automatically because no further action is required.

The Hardware Messages window displays the hardware messages for the selected object. If more than one object or a group of objects was selected, a tab on the right side of the window is available for each object. Messages are listed from the oldest to the newest message, with the oldest message displayed at the top of the list.

For information about changing the background color of the object icons to indicate that messages are pending, see “Hardware Management Console Settings” on page 106.

To display the **Hardware Messages**:

1. Open **Groups** from the **Views** area.
2. Select the group object that has a blue background.
3. Drag and drop the selected object on **Hardware Messages** in any task area.
4. The Hardware Messages window opens.

Online Help is available if you need additional information for viewing or deleting hardware messages.

Operating System Messages



Displays consolidated operating system generated messages for all selected CPC images. The operating system messages are displayed when one or more CPC image objects, or a group of CPC images, is dragged and dropped on the Operating System Messages icon. These messages are available to all default user IDs.

Note: Depending on your user task role, you may only view the operating system messages.

Coupling Facility Control Code (CFCC) commands can be sent from the Hardware Management Console to a CF when a CPC image that represents a CF is dragged and dropped on the Operating System Messages icon. To send a command, click **Send Command**.

For more information about the CFCC commands and messages, see the online books, *Coupling Facility Control Code Commands* and *Coupling Facility Control Code Messages*.

To display the **Operating System Messages**:

1. Open **Groups** from the **Views** area.
2. Select the desired CPCs or images.
3. Drag and drop the selected group on **Operating System Messages** in any task area.
4. The Operating System Messages window opens.

Online Help is available if you need additional information for viewing or deleting operating system messages.

Books



Display the Books view by double-clicking with the left mouse button on the Books icon in the *Views* area. Object icons representing the following online books provided with the Hardware Management Console are displayed in the *Books Work Area*

Note: If you are accessing the Hardware Management Console remotely, a PDF version of the document is available. If you are accessing the Hardware Management Console locally, an HTML version of the document is available.

Coupling Facility Control Code Commands: This publication is available exclusively as an online book. It provides information about commands you can issue from the Support Element to coupling facility control code.

Coupling Facility Control Code Messages: This publication is available exclusively as an online book. It provides information about messages sent from coupling facility control code to the Support Element.

Hardware Management Console Operations Guide: This online book is the publication you are currently using. It provides information about monitoring your system using the Hardware Management Console.

Hardware Management Console Operations Guide for Ensembles: This online book is a publication that describes the ensemble tasks you can use on the Hardware Management Console (HMC). It is used in conjunction with the *Hardware Management Console Operations Guide*.

To open an online book:

1. Open **Books** from the **Views** area.
2. In the **Books Work Area**, locate the book you want to open and double-click on the book icon. The book remains open until you close it
3. When you are finished viewing the book, close it by clicking the **X** in the upper right corner.

Support Element Operations Guide: This online book is a publication that provides information about the Support Element console application and about using the Support Element workplace to monitor and operate your system. To open this online book, see “Support Element Operations Guide” on page 170.

The following publications have been removed from the classic style user interface, however, they can be accessed from the Welcome window when you are using the tree style user interface.

- ***Application Programming Interfaces:*** This online book provides information to customers in developing system management applications that will provide integrated hardware and software system management solutions using the application programming interfaces.
- ***Application Programming Interfaces for Java:*** This online book describes the **com.ibm.hwmca.api** package. The purpose of this package is to allow Java applications, local or remote, the ability to exchange data related to the objects that the Console application manages.
- ***Common Information Model (CIM) Management Interface:*** This online book provides system programmers with instructions on how to manage their systems using Common Information Model (CIM) management interfaces on the Hardware Management Console.

Help



Display the Help view by double-clicking the left mouse button on the Help icon in the *Views* area. Information is provided about the tasks on the Hardware Management Console. To view all of the online help information:

1. Open **Help** from the **Views** area.
2. The **Help** window is displayed. On the left side of the window, the **Contents** area is displayed. You can select an item in the Contents and then select a specific task that you are interested in viewing the Help information. As you select a task, the help information for that task is displayed on the right side of the window.

You can also get to the help information for each task by clicking **Help** on the task window you are currently working in. The Help window opens with the Contents on the left and the help content on the right.

Chapter 5. Hardware Management Console tasks

This chapter describes the console tasks that are available on the Hardware Management Console.

To open these tasks using the classic style user interface, see “Console actions” on page 73, or if you are using the tree style user interface, see “HMC Management” on page 30 and “Service Management” on page 32.

Note: If you cannot access these tasks, contact your Access Administrator. You can also refer to Table 2 on page 203 for a list of the Hardware Management Console tasks and the corresponding predefined user IDs that can perform these tasks.

Analyze Console Internal Code



This task enables you to retrieve, delete, or view a Hardware Management Console internal code fix provided by IBM Product Engineering.

To analyze console internal code:

1. Open the **Analyze Console 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 (DVD-RAM, CD-ROM, or USB flash memory drive) or an FTP site. (See “USB flash memory drive” on page 10 for more information.)
 - 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**.

Use the online Help to get additional information on working with an internal code change.

Archive Security Logs



Notes:

- The DVD-RAM or USB flash memory drive used for archiving security logs must be formatted with a volume label of **ACTSECLG**.
- If you are using a USB flash memory drive it must have a capacity of 1 GB or greater.
- You cannot perform this task remotely.

This task allows you to archive a security log for the console. When the Archive Security Logs window is displayed, verify that the console shown in the window list is the one whose security log you want to archive.

To archive a security log:

1. Open the **Archive Security Logs** task. The Archive Security Logs window is displayed.
2. Verify the console shown in the window list is the one whose security log you want to archive.

Note: Ensure that the DVD-RAM or USB flash memory drive that you are using for archiving is inserted properly. (See “USB flash memory drive” on page 10 for more information.)

3. Click **Archive**, choose the mass rewritable media (DVD-RAM or USB flash memory drive) to archive to from the Select Media Device window, then click **OK** to start the procedure.

Use the online Help if you need additional information for archiving a console security log.

Audit and Log Management



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. For example, the User profiles data type is displayed only to users who are authorized to use the **User Profiles** task.

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.

Use the online Help to get additional information on generating audit report data.

Authorize Internal Code Changes



This task gives you the option to allow or to not allow the Hardware Management Console and its defined CPCs to install and activate licensed internal code changes.

To authorize internal code changes:

1. Open the **Authorize Internal Code Changes** task. The Authorize Internal Code Changes window is displayed.

2. To authorize internal code changes make sure **Do not allow installation and activation of internal code changes** is *not* selected (a check mark does not appear).
3. Click **Save** if a change was made and begin the operation, or **Cancel** to close the task without proceeding with the operation.

Use the online Help to get additional information about enabling or disabling the setting for internal code change authorization.

Backup Critical Console Data



Notes:

- The USB flash memory drive used for the **Backup Critical Console Data** task must be formatted with a volume label of **ACTBKP**.
- This task backs up only the critical data associated with Hardware Management Console Application (HWMCA).
- To back up data stored on each Support Element, see “Backup Critical Data” on page 153.

This task backs up the data that is stored on your Hardware Management Console hard disk and is critical to support Hardware Management Console operations. You should back up the Hardware Management Console data after changes have been made to the Hardware Management Console or to the information associated with the processor cluster.

Information associated with processor cluster changes is usually information that you are able to modify or add to the Hardware Management Console hard disk. Association of an activation profile to an object, the definition of a group, hardware configuration data, and receiving internal code changes are examples of modifying and adding information, respectively.

Use this task after customizing your processor cluster in any way. A backup copy of hard disk information may be restored to your Hardware Management Console following the repair or replacement of the fixed disk.

To back up console data:

1. Open the **Backup Critical Console Data** task. The Backup Critical Console Data Confirmation window is displayed.
2. Insert the backup USB flash memory drive, then click **Backup** to begin. (See “USB flash memory drive” on page 10 for more information.)
3. The Backup Critical Console Data Progress window is displayed.
4. When backup is complete, click **OK**.

Use the online Help if you need additional information for backing up the Hardware Management Console data.

Block Automatic Licensed Internal Code Change Installation



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.

Use the online Help to get additional information about blocking or unblocking automatic licensed internal code installations.

Certificate Management



All remote browser access to Version 2.9.0 or later of the Hardware Management Console must use Secure Sockets Layer (SSL) encryption. With SSL encryption required for all remote access to the Hardware Management Console, a certificate is required to provide the keys for this encryption. Version 2.9.0 or later of the Hardware Management Console provides a self-signed certificate that allows this encryption to occur.

This task manages the certificate(s) used on your Hardware Management Console. It provides the capability of getting information on the certificate(s) used on the console. This task allows you to create a new certificate for the console, change the property values of the certificate, and work with existing and archived certificates, signing certificates, or cipher suites.

Note: For any newly created, self-signed, or CA-signed certificates, the supported certificate key length is 2048 bits.

To manage your certificates:

1. Open the **Certificate Management** task. The Certificate Management window is displayed.
2. Use the menu bar from the Certificate Management window for the actions you want to take with the certificates:
 - To create a new certificate for the console, click **Create**, then select **New Certificate**. Determine whether your certificate will be self-signed or signed by a Certificate Authority, then click **OK**.
 - To modify the property values of the self-signed certificate, click **Selected**, then select **Modify**. Make the appropriate changes, then click **OK**.
 - To work with existing and archived certificates, signing certificates, or cipher suites, click **Advanced**. Then you can choose the following options:
 - Delete and archive certificate
 - Work with archived certificate
 - Import server certificate
 - Manage trusted signing certificates
 - View issuer certificate.
3. Click **Apply** for all changes to take effect.

Use the online Help if you need additional information for managing your certificates.

Change Console Internal Code



This task enables you to specify what you want to do with the internal code changes provided by IBM. This function is used when working with the Licensed Internal Code supplied with the Hardware Management Console. For information on changes to an object's internal code, see “Change Internal Code” on page 161.

An IBM service representative will provide new internal code changes and manage their initial use. For internal code changes already stored on your Hardware Management Console hard disk, IBM recommends that you manage these changes only under the supervision of an IBM service representative or with the assistance of your IBM Service Support System. Licensed internal code controls many of the operations available on the Hardware Management Console. Internal code changes may provide new operations, or correct or improve existing operations.

To change the internal code on the Hardware Management Console:

1. Open the **Change Console Internal Code** task. The Change Console Internal Code window is displayed.
2. Select one of the following options for managing the internal code, then click **OK**.

Note: Verify that the term **Enabled** is displayed in the **Change Management Services** field. Change management services must be enabled for you to use options that manage the internal code changes stored on the Hardware Management Console hard disk.

- Accept installed changes that were activated
- Check dependencies
- Install and activate changes that were retrieved
- Browse system and internal code information
- Remove and activate changes
- Retrieve internal code changes
 - If you select the **Retrieve code changes from the IBM support system to removable media** option, you will need to specify an IBM Server Support System (RETAIN) user ID and password to continue.
 - If you select the **Retrieve changes from FTP site to the Hardware Management Console** option, you will need to provide FTP site access information and you have the option to enable a secure data transfer.
- Delete retrieved changes that were not installed

If you select the **Retrieve internal code changes** option and then

Use the online Help if you need additional information about working with an internal code change.

Change Password



Note: If you are logged onto the Hardware Management Console using an LDAP user ID, this task is not available.

This task allows you to change your password.

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 **OK** to change your password.

Use the online Help if you need additional information for changing your password.

Configure 3270 Emulators



Note: You cannot perform this task remotely.

This task configures the Hardware Management Console to automatically start one or more 3270 emulator sessions when the Hardware Management Console application starts.

A 3270 emulator is an application that allows 3270 terminal emulation from the Hardware Management Console to a host operating system. When configuring a 3270 emulator, you must specify the TCP/IP address of the target system.

To configure 3270 emulators:

1. Open the **Configure 3270 Emulators** task. The Configure 3270 Emulators window is displayed.
2. From this window you can add a new host address, delete an existing host address, or start a 3270 host emulator session.
3. Click **OK** to save your changes.

Use the online Help to get additional information for configuring a 3270 emulator session.

Configure Data Replication



Note: If you are using the classic style user interface, this task is found under the **Hardware Management Console Settings** console action.

This task, used by an access administrator or a user ID that is assigned access administrator roles, enables or disables customized data replication. Customized data replication allows another Hardware Management Console to obtain customized console data from or send data to this Hardware Management Console.

Note: Customizable console data is accepted from other Hardware Management Consoles only after specific Hardware Management Consoles and their associated allowable customizable data types have been configured.

For more detailed information on customizing console data for data replication, see Appendix G, “Customizable data replication,” on page 243. You can also use the online Help to get additional information for enabling or disabling customizable data replication.

Console Default User Settings



This task, used by an access administrator or a user ID that is assigned access administrator roles, customizes the default appearance and behavior of the interface for the users of the Hardware Management Console workplace.

To set the default user settings for the Hardware Management Console:

1. Open the **Console Default User Settings** task. The Console Default User Settings window is displayed.
2. Proceed through the tabs to customize the user settings:
 - **Tree Style** - customizes the tree style user interface appearance
 - **Classic Style** - customizes the classic style user interface appearance
 - **Confirmations** - customizes the preferences for using confirmation windows for a subset of console workplace tasks
 - **Colors and Patterns** - sets the colors (or patterns) for indicating exceptions when using the classic style user interface only
 - **Controls** - selects object controls
 - **UI Style** - sets the user interface and determines whether or not the users are allowed to switch the user interface style
3. Click **Apply** to save the settings currently displayed or changed, or
Click **Reset** to discard any changes you made to the settings after you opened this task and redisplay the current settings, or
Click **Defaults** to discard any changes you made to the settings at any time and redisplay the original default settings that were provided with this version of the Hardware Management Console.
4. Click **OK** when you have completed the task.

Use the online Help if you need additional information for customizing the default settings.

Console Messenger



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.

This task is used to provide a simple person-to-person message communication facility between users of the Hardware Management Console and the Support Element.

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.

If you select a top level console from *Reachable Consoles* that is a Support Element, the *Message Type* displays **Broadcast** and an additional option, **In addition, send the message to all managing consoles.**, is displayed. This option controls the distribution of the message. Broadcast messages are always sent to all of the users on the selected console. However, if you select this option the broadcast message is also sent to all users on all Hardware Management Consoles that are acting as managing consoles of the Support Element. This option is not available when the selected console is a Hardware Management Console.

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 Hardware Management Console workplace.

If you are receiving a broadcast message, the Broadcast Message Received window is immediately displayed on your Hardware Management Console screen. 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 Hardware Management 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 the chat window comes to the foreground in your Hardware Management Console sessions when partners send you messages, select **Bring chat window to foreground on message arrival**. (a check mark appears).

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 Hardware Management 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.

Use the online Help if you need additional information for sending and receiving two-way chats and broadcast messages to this console and remote consoles.

Copy Console Logs to Media



Note: You cannot perform this task remotely.

This task copies the Hardware Management Console log file (**IQYYLOG.LOG**) to a media device (DVD-RAM, USB flash memory drive, or diskette (if one is available)). You may want to do this for saving or archiving the log file. (See “USB flash memory drive” on page 10 for more information.)

To copy the log file to a media device:

1. Open the **Copy Console Logs to Media** task. Insert the media device that you want to copy the console logs to. The Select Media Device window is displayed.
2. Select the media device, then click **OK**.
3. Follow the instructions on the subsequent windows to complete the task.

Use the online Help if you need additional information for copying console logs to media.

Create Welcome Text



This task, used by an access administrator or a user ID that is assigned access administrator roles, allows you to customize the welcome message or display a warning message that appears on the Welcome window before you log onto the Hardware Management Console. You can use this text to notify users of certain corporate policies or security restrictions applying to the system.

To create a message:

1. Open the **Create Welcome Text** task. The Create Welcome Text window is displayed.
2. Enter a message in the input field to be displayed in the Welcome window. You can also specify a label name in the **Classification** input field that will be displayed as the background on the Welcome and Logon windows.
3. Click **OK** to apply the change.
4. The next time you log on to the Hardware Management Console your message is displayed.

Use the online Help to get additional information about displaying a message before logging onto the Hardware Management Console.

Customize API Settings



Note: If you are using the classic style user interface, this task is found under the **Hardware Management Console Settings** console action.

This task, used by an access administrator or a user ID that is assigned access administrator roles, allows you to control Hardware Management Console Application Programming Interfaces (APIs) access. This access permits applications that were not supplied as part of the Hardware Management Console Application (HWMCA) to communicate with the objects defined to this Hardware Management Console.

- | 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. You can enable or disable the Web
- | Services Application Programming Interface (API) from the **WEB Services** tab. You can also enable or disable the Common Information Model (CIM) interface from the **CIM** tab.
- | For more information on SNMP, Web Services and CIM APIs, see *Application Programming Interfaces*, SB10-7030, *Hardware Management Console Web Services API*, SC27-2616, and *Common Information Model (CIM) Management Interface*, SB10-7154, respectively.

To customize API settings:

1. Open the **Customize API Settings** task. The Customize API Settings window is displayed.
2. From the **SNMP** tab you can enable SNMP APIs and add, change, or delete community names, SNMPv3 users, and event notification information. From the **WEB Services** tab you can enable or disable the Web Services Application Programming Interface (API) and control the IP addresses and user access. From the **CIM** tab you can enable or disable the CIM interface.
3. Click **OK** to save the SNMP, WEB Services, or CIM configurations and continue.

Use the online Help to get additional information about customizing API settings.

Customize Auto Answer Settings



Note: If you are using the classic style user interface, this task is found under the **Hardware Management Console Settings** console action.

This task configures the settings to allow the Hardware Management Console to automatically answer an incoming telephone call to the attached modem. You define the login name and password to use for a Point-to-Point Protocol (PPP) dial-up connection to a Hardware Management Console. The Hardware Management Console uses the PPP protocol to control which users can establish incoming connections. A user who wants to establish a dial-up connection to call and connect to a Hardware Management Console must use this login name and password when configuring the dial-up client. For example, a user trying to connect to a Hardware Management Console from a Windows system uses this login name and password, which establishes a Windows Dial-up Networking configuration for calling a particular Hardware Management Console. See “Using Windows XP to dial to a Hardware Management Console” on page 220 for more information.

To customize automatic call answer settings:

1. Open the **Customize Auto Answer Settings** task. The Customize Automatic Call Answer Settings window is displayed.
2. Select **Enable automatic call answering**, then provide the appropriate information for the input fields.
3. Click **OK** to save the information and exit the task.

Use the online Help to get additional information about customizing auto answer settings.

Customize Automatic Logon



Note: If you are using the classic style user interface, this task is found under the **Hardware Management Console Settings** console action.

This task, used by an access administrator or a user ID that is assigned access administrator roles, enables or disables the automatic logon feature.

When enabled, the automatic logon feature will log on the Hardware Management Console automatically using the user ID you specified whenever the Hardware Management Console is powered on.

To customize automatic logon:

1. Open the **Customize Automatic Logon** task. The Customize Automatic Logon window is displayed.
2. Select **Enable automatic logon feature**, then select a user ID.
3. Click **OK** to save the setting and exit the task.

Use the online Help to get additional information for setting up automatic logon.

Customize Console Date/Time



This task enables you to change the time and date of the battery operated Hardware Management Console clock and allows you to set up a Network Time Protocol (NTP) client.

The battery operated clock keeps the time and date for the Hardware Management Console. You can change the settings of the battery operated clock:

- If the battery is replaced in the Hardware Management Console.

- If your system is physically moved to a different time-zone.

An attempt is made every night to synchronize the Hardware Management Console clock with a CPC that has been enabled for time synchronization. If a CPC is enabled for time synchronization (using the **Change Object Definition** or **Add Object Definition** tasks), this task causes the Hardware Management Console to update its clock with the time that is set on the CPC Support Element and keyboard entries will be ignored.

The following list shows the zone correction for some major cities around the world:

City	Direction	Number of Hours Standard Time	Number of Hours Daylight Time
Amsterdam	East	1	2
Anchorage	West	9	8
Berlin	East	1	2
Buenos Aires	West	3	-
Chicago	West	6	5
Denver	West	7	6
London	East	0	1
Los Angeles	West	8	7
New York City	West	5	4
Madrid	East	1	2
Oklahoma City	West	6	5
Paris	East	1	2
Pittsburgh	West	5	4
Rio de Janeiro	West	3	-
Rome	East	1	2
Stockholm	East	1	2
Sydney	East	10	11
Tel Aviv	East	2	3
Tokyo	West	9	-
Toronto	West	5	4
Vienna	East	1	2

For the procedure for changing the Hardware Management Console date and time, see Appendix F, “Changing your time-of-day clock,” on page 239. You can also use the online Help if you need additional information.

This task also allows you to set up a Network Time Protocol (NTP) client.

Note: When the Hardware Management Console is configured to have an NTP client running, the Hardware Management Console is continuously synchronized to an NTP server instead of synchronizing to a Support Element at a specific time. When the NTP client is no longer running and if a Hardware Management Console is set up to synchronize to a Support Element, the synchronization is requested immediately when the NTP client has stopped and then the Hardware Management Console will synchronize with the Support Element at the designated time.

To set up the configuration for the NTP client:

1. Open the **Customize Console Date/Time** task. The Customize Console Date and Time window is displayed.
2. Select the **Configure NTP Settings** tab. From this page you can set up the configuration of the NTP client.
3. Click **Add NTP Server...** to add a server to the NTP configuration file. The Add a Network Time Server window is displayed.
4. Specify a time server host name or IP address and select the NTP protocol version, then click **OK**.

Note: To locate an external NTP server, you can:

- Use the Internet to search for Network Time Protocol.

- See <http://www.ntp.org> for a list of public servers as well as a list of NTP “pools” that allows the console to get the NTP time from a server that is in the pool. For example, in the United States, you can specify the following addresses:
 - 0.us.pool.ntp.org
 - 1.us.pool.ntp.org
 - 2.us.pool.ntp.org
 - 3.us.pool.ntp.org
- 5. Select **Enable NTP service on this console** to allow this console to obtain the current date and time from any of the NTP servers that are listed.
- 6. Select **Enable this Hardware Management Console to act as a time server** to allow this console to become an NTP server which in turn allows another console to obtain the current date and time from this Hardware Management Console.
- 7. Click **OK** when you have completed this task, or click **Cancel** to exit the without making any changes.

Use the online Help to get additional information for setting up the NTP client or see “ETS configuration” on page 233.

Customize Console Services



Note: If you are using the classic style user interface, this task is found under the **Hardware Management Console Settings** console action.

This task enables or disables Hardware Management Console services. A Hardware Management Console service is a facility or function of the Hardware Management 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 operation

Controls whether this Hardware Management Console can be operated using a web browser from a remote workstation. See Appendix C, “Remote operations,” on page 215 for more information.

Note:

- The tasks that require removable media cannot be performed remotely.
- This option is not available if you are accessing the Hardware Management Console remotely.

Remote restart

Controls whether this Hardware Management Console can be restarted by a user accessing it from a remote workstation. If this service is Disabled, only local users at this Hardware Management Console can use the **Shutdown or Restart** task.

LIC change

Controls whether this Hardware Management Console provides change management operations for its defined objects and for other Hardware Management Consoles.

Optical error analysis

Controls whether this Hardware Management Console analyzes and reports optical problems for its defined objects. (Optical problems are problems occurring on ESCON or coupling facility channel links.)

CIM management interface

Note: This option is no longer enabled from this task. Use the **Customize API Settings** task to enable or disable the CIM management interface.

Controls whether this Hardware Management Console can be remotely managed using the Common Information Model (CIM) interface.

Console messenger

Controls whether the console messenger facility is active on this Hardware Management Console or not. The console messenger facility allows users of this Hardware Management Console to send and receive instant messages and broadcast messages to other users of this console and remote consoles.

Fibre channel analysis

Controls whether this Hardware Management Console analyzes and reports fibre channel problems. (Fibre channel problems are problems occurring on FICON channel links.)

Large retrieves from RETAIN

Controls whether this Hardware Management Console can retrieve internal code changes from RETAIN for engineering change streams that are expected to contain a large amount of data.

To enable or disable Hardware Management Console 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.

Use the online Help to get additional information for enabling or disabling Hardware Management Console services.

Customize Customer Information

**Notes:**

- If Customizable Data Replication is **Enabled** on this Hardware Management Console (using the **Configure Data Replication** task), the data 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” on page 86.
- If you are using the classic style user interface, this task is found under the **Hardware Management Console Settings** console action.

This task enables you to customize the customer information for the Hardware Management Console.

To customize your customer information:

1. Open the **Customize Customer Information** task. The Customize Customer Information window is displayed.
2. Select one of the following tabs from the **Customize Customer Information** window.
 - Administrator
 - System
 - Account.
3. Supply the appropriate information in the fields provided.
4. Click **OK** when you have completed the task.

Use the online Help to get additional information about customizing your account information.

Customize Modem Settings



Notes:

- If Customizable Data Replication is *Enabled* on this Hardware Management Console (using the **Configure Data Replication** task), the data 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” on page 86.
- If you are using the classic style user interface, this task is found under the **Hardware Management Console Settings** console action.

This task configures the basic modem settings for remote support. These settings include:

Dial type

Tone for touch-tone phones or pulse for rotary phones.

Other settings

Sets whether to wait for dial tone, whether to enable speaker, and any dial prefix (number to dial before dialing external numbers).

To enable or disable modem settings:

1. Open the **Customize Modem Settings** task. The Customize Modem Settings window is displayed.
2. Select the dial type and the other settings you prefer.
3. Click **OK** to complete the task.

Use the online Help to get additional information for configuring the basic modem settings.

Customize Network Settings



Notes:

- If Customizable Data Replication is *Enabled* on this Hardware Management Console (using the **Configure Data Replication** task), the data 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” on page 86.
- If you are using the classic style user interface, this task is found under the **Hardware Management Console Settings** console action.

This task allows you to view the current network information for the Hardware Management Console and to change the network settings as shown in the following list.

Identification

Contains the host name and domain name of the Hardware Management Console.

Console name

Your Hardware Management 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:

hmcibm1

Domain name

An alphabetic name that Domain Name Services (DNS) can translate to the IP address. For example, DNS might translate the domain name 222.example.com to 198.105.232.4. The long host name consists of console name plus a period plus a domain name, for example:

hmcibm1.endicott.ibm.com

Console description

This description is for your use only. An example might be:

Main Hardware Management 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.

Basic Settings

This tab allows you to view and change current LAN adapter settings for your console, specifically for IPv4 addresses. This page also allows you to indicate that an IPv4 address is not available.

IPv6 Settings

This tab allows IPv6 configuration settings for the selected network adapter defined on this console. An IPv6 address is always available locally (within the subnet defined).

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 Hardware Management Console where to send data if the target station does not reside on the same subnet as this Hardware Management Console. This information is needed to allow the Hardware Management Console to connect to IBM Service Support System 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: The order of the entries in the "Routing Information" table is significant. The destination IP address of each outgoing packet will be matched against these entries in order from first to last; the gateway of the first matching entry will be used for routing that packet. The order of the entries can be controlled when adding the rules. You must first select an existing entry in the table (if one exists), then you can choose to add the new rule before or after the selected rule. In general, entries should be added in order of decreasing netmask length.

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.

Use the online Help to get additional information for customizing the network settings.

Customize Outbound Connectivity



Notes:

- If Customizable Data Replication is **Enabled** on this Hardware Management Console (using the **Configure Data Replication** task), the data 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” on page 86.
- If you are using the classic style user interface, this task is found under the **Hardware Management Console Settings** console action.
- See Appendix D, “Remote support facility,” on page 223 for information about the connectivity methods available for remote support and guidance on setting up connectivity to IBM service.

This task allows you to customize the means for outbound connectivity for the Hardware Management Console to use to connect to remote service. You can configure this Hardware Management Console to attempt connections through the Internet or through the local modem or both. Remote service is a two-way communication between the Hardware Management Console and the IBM Service Support System for conducting automated service operations. The connection can only be initiated by the Hardware Management Console. The IBM Service Support System never attempts to initiate a connection to the Hardware Management Console.

Before you can customize the means for outbound connectivity for the Hardware Management Console, you must first decide which Hardware Management Consoles will handle call-home requests initiated by this Hardware Management Console.

1. Open the **Customize Outbound Connectivity** task. The Call-Home Server Consoles window is displayed.
2. You can click **Configure...** to configure this console as a local call-home server and to identify the connectivity method it uses to connect to the service provider. The Outbound Connectivity Settings window is displayed.

Or, before you configure the local Hardware Management Console you can identify additional call-home server consoles that might also handle the call-home requests initiated by this Hardware Management Console. Click **Add...** to provide another IP address or host name, then click **Configure...** to continue with the task.

Use the online Help to get additional information about identifying the call-home server consoles.

3. Click **Cancel** to end this task without making changes, otherwise continue customizing outbound connectivity settings.

To customize your connectivity information from the Outbound Connectivity Settings window:

1. Select **Enable the local console as a call-home server** (a check mark is displayed) before proceeding with the task.
2. The Outbound Connectivity Settings window displays the following tabs for providing input:
 - Local Modem
 - Internet (this can be either a direct internet connection or an indirect connection using a customer-supplied SSL proxy)
 - External Time Source
3. Use the **Local Modem** tab if you want to allow connectivity over a modem, then select **Allow local modem dialing for service** (a check mark is displayed).
 - a. If your location requires a prefix to be dialed in order to reach an outside line, click **Modem Configuration...** and enter the **Dial prefix** in the Customize Modem Settings window required by your location. Click **OK** to accept the setting.

- b. Click **Add...** from the **Local Modem** tab page to add a telephone number. (The **Add Telephone Number** window is displayed.) When local modem dialing is allowed, there must be a telephone number configured.
4. Use the **Internet** tab if you want to allow connectivity over the Internet. Select **Allow an existing internet connection for service** (a check mark is displayed) to be able to perform call-home functions over an encrypted SSL connection. The following information must be properly configured from the **Customize Network Settings** task:
 - a. To enable using an SSL proxy to access the Internet, select **Use SSL proxy**. If you select **Use SSL proxy**, you must provide an internet protocol address and port number to direct requests. The internet protocol address can be specified as either a host name or TCP/IP address (IPv4 or IPv6 format).
 - b. If your proxy requires authentication to forward requests, select **Authenticate to the SSL proxy** and enter the user name and password that is used for all requests called home from this Hardware Management Console.

Notes:

- The Hardware Management Console must have a Local Area Network (LAN) adapter that is connected to a network with Internet access. This can be a direct internet connection, or an internet connection from an SSL proxy.
- The LAN adapter must be configured with a default gateway that provides access to the Internet (or SSL proxy).
- If a firewall is in place between the Hardware Management Console and the Internet, it must allow outgoing TCP/IP connections on port 443 from the Hardware Management Console to your service provider. The IP addresses you must allow depends on the protocol you choose on the **Protocol to Internet** selection field for this task:
 - For Hardware Management Consoles at Version 2.9.2 or earlier, you must allow access to the following IPv4 addresses:
 - 129.42.160.48 and 207.25.252.200 (allow Hardware Management Console access to System Authentication Server (SAS))
 - 129.42.160.49 and 207.25.252.204 (allow Hardware Management Console access to IBM Service for North or South America)
 - 129.42.160.50 and 207.25.252.205 (allow Hardware Management Console access to IBM Service for all other regions)

Note: You only need to specify the IP address necessary to set up access to SAS and those appropriate for your region.

- For Hardware Management Consoles at Version 2.10.0 or later, internet connectivity to the IBM Service Support System has been enhanced to enable access from the IPv6 internet in addition to the IPv4 internet. If you require access to the IBM Service Support System using the IPv6 internet, you must allow access to all these additional addresses:
 - 2620:0:6C0:1::1000
 - 2620:0:6C1:1::1000
 - 2620:0:6C2:1::1000
- For Hardware Management Consoles at Version 2.10.1, Internet Protocol addresses using IPv4 requires outbound connectivity to the following IP addresses:
 - 129.42.26.224
 - 129.42.34.224
 - 129.42.42.224

If your Hardware Management Console connects to the Internet using IPv6, use the preceding definitions.

5. Use the **External Time Source** tab if you want to set up the modem parameters to be used when dialing an External Time Source (ETS) in support of CPCs that are participating in an STP-only Coordinated Timing Network (CTN), then select **Allow external time source dialing using the local modem** (a check mark is displayed).
 - a. If your location requires a prefix to be dialed in order to reach an outside line, click **Modem Configuration...** and enter the **Dial prefix** in the Customize Modem Settings window required by your location. Click **OK** to accept the setting.
 - b. Select one of the time services listed.
 - c. Click **Add...** from the **External Time Source** tab page to add a telephone number. When external time source dialing is allowed, there must be at least one telephone number configured.
6. When you complete all the necessary fields, click **OK** to save your changes.

Use the online Help if you need additional information for customizing outbound connectivity information and see Appendix D, "Remote support facility," on page 223.

Customize Product Engineering Access



Note: If you are using the classic style user interface, this task is found under the **Hardware Management Console Settings** console action.

This task, used by an access administrator or a user ID that is assigned access administrator roles, enables or disables the authorization of IBM Product Engineering access to the Hardware Management Console. Once product engineering is enabled to access the Hardware Management Console you can decide whether or not product engineering can access the system remotely.

With access authority, IBM Product Engineering can log on the Hardware Management 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 Hardware Management 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.

Use the online Help to get additional information for customizing product engineering access to your Hardware Management Console.

Customize Remote Service



Notes:

- If Customizable Data Replication is **Enabled** on this Hardware Management Console (using the **Configure Data Replication** task), the data 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” on page 86.
- If you are using the classic style user interface, this task is found under the **Hardware Management Console Settings** console action.

This task allows you to customize the Hardware Management Console for using remote service. **Remote service** is two-way communication between the console and the IBM Service Support System (commonly known as RETAIN) for 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 connection can only be initiated by the Hardware Management Console. The IBM Service Support System never attempts to initiate a connection to the Hardware Management Console. Some examples for enabling remote service:

- Allows the Hardware Management Console to automatically report a problem and request service through the IBM Service Support System
- Uses the IBM Service Support System as a source for retrieving internal code changes and as a destination for transmitting service data.

When remote service is disabled, error information and requests for service must be done through voice communications.

To configure remote service:

1. Open the **Customize Remote Service** task. The Customize Remote Service window is displayed.
2. Select **Enable remote service requests**. This option allows the Hardware Management Console to establish remote connections to the IBM Service Support System.
3. To enable automatic service calling for System z problems, select **System z**. This option allows the Hardware Management Console to automatically report problems and get service through its remote connection to the IBM Service Support System.

If the IBM zEnterprise BladeCenter Extension (zBX) feature is installed then you also have the option to select **zBX** to set the Hardware Management Console for authorization to automatically report zBX problems that require service. For additional zBX information, see the *Hardware Management Console Operations Guide for Ensembles*.

4. After you enable remote service, you must customize the telephone number for calling the IBM Service Support System.
5. When you complete the necessary fields, click **OK** to save your changes.

Use the online Help if you need additional information for setting up remote service.

Customize Scheduled Operations



This task enables you to:

- Schedule an operation to run at a later time
- Define operations to repeat at regular intervals
- Delete a previously scheduled operation
- View details for a currently scheduled operation
- View scheduled operations within a specified time range
- Sort scheduled operations by date, operation, or console.

You can schedule the times and dates for automatic licensed internal code updates and backup of critical hard disk data for the Hardware Management Console. Using this task displays the following information for each operation:

- The processor that is the object of the operation.
- The scheduled date
- The scheduled time
- The operation
- The number of remaining repetitions.

An operation can be scheduled to occur one time or it can be scheduled to be repeated. You will be required to provide the time and date that you want the operation to occur. If the operation is scheduled to be repeated, you will be asked to select:

- The day or days of the week that you want the operation to occur. (optional)
- The interval, or time between each occurrence. (required)
- The total number of repetitions. (required)

The operations that can be scheduled for the Hardware Management Console are:

Single step code changes retrieve and apply

Schedules an operation to copy (retrieve) the Hardware Management Console internal code changes to the Hardware Management Console hard disk and then install (apply) the code changes.

Backup critical hard disk information

Schedules an operation to make a backup of critical hard disk information for the Hardware Management Console.

Accept internal code changes

Schedules an operation to make activated internal code changes a permanent working part of the licensed internal code of the Hardware Management Console.

Install and activate concurrent code changes

Schedules an operation for installing and activating internal code changes retrieved for the Hardware Management Console.

Remove and activate concurrent code changes

Schedules an operation for removing and activating internal code changes installed for the Hardware Management Console.

Note: After changes are accepted, they cannot be removed.

Retrieve internal code changes

Schedules an operation to copy internal code changes from a remote service support system to the Hardware Management Console hard disk.

Retrieve internal code changes for defined CPCs

Schedules an operation to copy internal code changes for Central Processor Complexes (CPCs) from a remote support system to the hard disk of the Support Element for each of the CPCs.

Transmit system availability data

Schedules a transmittal of system availability data from the Hardware Management Console to the Product Support System (PSS).

Audit and Log Management

Schedules an operation to generate an audit report on selected types of audit data.

To schedule operations on the Hardware Management Console from the Customize Scheduled Operations window, click **Options** from the menu bar to display the next level of menu options:

1. Open the **Customize Scheduled Operations** task. The Customize Scheduled Operations window is displayed.

2. Click **Options** from the menu bar to display the following menu options:
 - a. To add a scheduled operation, click **New...**
 - b. To delete a scheduled operation, select the operation you want to delete, then click **Delete**.
 - c. To return to the Hardware Management Console workplace, click **Exit**.
3. Click **View** from the menu bar to display the following menu options:
 - a. To view a scheduled operation, select the operation you want to view, point to **View** and then click **Schedule Details...**
 - b. To change the time of a scheduled operation, select the operation you want to view, point to **View** and then click **New Time Range...**
4. Click **Sort** from the menu bar to sort the scheduled operations, select a sort group that you prefer.
5. Use the online Help to get additional information for scheduling an operation.

Customize User Controls



Notes:

- If Customizable Data Replication is *Enabled* on this Hardware Management Console (using the **Configure Data Replication** task), the data 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” on page 86.
- Predefined roles (default roles) cannot be modified or removed.

This task, used by an access administrator or a user ID that is assigned access administrator roles, defines and customizes user roles. A *user role* is a collection of authorizations. A user role can be created to define the set of tasks allowed for a given class of user (*task roles*) or it can be created to define the set of managed objects that are manageable for a user (*managed resource roles*). Once you have defined or customized the user roles you can use the **User Profiles** task to create new users with their own permissions. (See “User Profiles” on page 124, for more information.)

To customize managed resource roles or task roles:

1. Open the **Customize User Controls** task. The Customize User Controls window is displayed.
2. Select either **Managed Resource Roles** or **Task Roles**.
3. Select the object you want to customize.
4. Click **Edit** from the menu bar to display the actions available.
5. Click **Add...**, **Copy...**, **Remove**, **Modify...**, or **Exit** depending on the task you want to perform.

You can also create user roles that have view only access for select tasks. The following view only tasks include:

- Hardware Messages
- Operating System Messages
- Customize/Delete Activation Profiles
- OSA Advanced Facilities
- Configure Channel Path On/Off

To create a user role that includes view only tasks:

1. Open the **Customize User Controls** task. The Customize User Controls window is displayed.
2. Select **Task Roles** and the task role you want to customize.
3. Click **Edit** from the menu bar to display the actions available.

4. Click **Add...** to create a new user role.
5. Select tasks from the Available Tasks group that you want the new user role to have access to. If the task is view only, the View Only Version Available message window is displayed. Click **Yes** if you want to add the view only version of that task for the user role you are creating.
6. When you have completed creating the new user role, click **OK**. From the **Edit** menu bar click **Exit** to close the task.

Use the online Help to get additional information for customizing managed resource roles and task roles.

Domain Security



This task provides a method for you to maintain the security of a processor complex by controlling the access of the Hardware Management Consoles to the CPC Support Elements. Hardware Management Consoles can only communicate with CPC Support Elements that have the same domain name and domain password as the Hardware Management Console. Assigning a unique domain name and password to a Hardware Management Console and the CPCs that are defined to it will isolate those CPCs from any other Hardware Management Console connected to the same Local Area Network (LAN).

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.

Use the online Help to get additional information for assigning a unique domain name and password.

Enable Electronic Service Agent



This task, used by an access administrator or a user ID that is assigned access administrator roles, provides a dialog to enable Electronic Service Agent functions and to set up or change certain parameters associated with the function of Electronic Service Agent.

This task is for any z/OS® user that is interested in the Electronic Services for zSeries and for those z/OS users that plan to install the z/OS product *IBM Electronic Service Agent for IBM zSeries and IBM S/390®, Version 1 Release 2 Modification Level 0, program number 5655-F17*. For more information about Electronic Services and Electronic Service Agent see the main website, <https://www.ibm.com/support/electronic>, and for all documentation you can see the FTP site, <ftp://ftp.software.ibm.com/s390/serviceagent>.

The Electronic Service Agent (program number 5655-F17) may be enabled to collect information from the system environment, including:

- IBM I/O device error data
- IBM software inventory and PTF levels
- Hiper/PE report requests.

When enabled by you, this function collects selected I/O error reports and analyzes them, reporting severe errors and requesting service when appropriate. I/O statistical data and customer system configuration data and system measurement data are transmitted to IBM periodically. IBM maintains the collected data on its servers in support of service related activities and generates information for you to use in helping manage the service and growth of your system. IBM may share the data with our services, support, development, and marketing teams. IBM will ensure that the collected data is available only to those parties who have a legitimate need-to-know.

To enable or disable the Electronic Service Agent function:

1. Open the **Enable Electronic Service Agent** task. The Electronic Service Agent License Agreement window is displayed.
2. First, you can either agree with the license and continue with the configuration or disagree and disable the function entirely.
3. If you agree with the terms stated in the license description, click **I Agree**. If you do not agree, the Electronic Service Agent cannot be enabled and the dialog will end.
4. When you agree, the Data Selection window is displayed allowing you to:
 - Select the data types that are to be allowed
 - Set the FTP user ID and password that must be used for all z/OS Service Agent transactions to transfer data to this Hardware Management Console

Note: This dedicated FTP user ID is used only by z/OS Electronic Service Agent clients. It has limited access and can only access dedicated separate partitions and directories on the Hardware Management disk. The dedicated directory is used by z/OS Service Agent clients to temporarily store collected data before it is sent to IBM. Its limited authorization for what it can do only includes transferring data to the Hardware Management disk and getting response files back to the client, with a response message indicating if the data was successfully sent to IBM or not.

- Set up the necessary local firewall rules to control which external systems are to be allowed FTP access for Electronic Service Agent
 - Set the time of day when the daily transfers of Electronic Service Agent data to IBM are to be initiated.
5. If you elect to add firewall rules for specific z/OS TCP/IP addresses, you must de-select **Allow FTP access from any address** and click **Add** for individual addresses.
 6. After all selection and data fields are complete, click **OK** to save the data and complete the enablement of Electronic Service Agent.

You may re-enter or change these selections at any time by executing this function.

In addition to enabling the Electronic Service Agent using this task you may also be interested in setting up a separate LAN connection to be used specifically with the z/OS systems where the Service Agent will be activated. See the **Customize Network Settings** task for setting up another LAN adapter and IP subnet mask so you can connect the systems in the network where the Service Agent FTPs data to the dedicated directory of the Hardware Management Console.

Use the online Help if you need additional information for enabling or disabling Electronic Service Agent.

Enable FTP Access to Mass Storage Media



This task allows your system processor to install software from mass storage media (CD, DVD, or USB flash memory drive) located on the Hardware Management Console. In addition to using this task you also need to work with the **Load from Removable Media or Server** task and monitor Operating System Messages. See Appendix H, “Installing software from a mass storage device,” on page 249 for the entire procedure and see “USB flash memory drive” on page 10 for more information on the USB flash memory drive.)

To allow FTP access to the mass storage media:

1. Open the **Enable FTP Access to Mass Storage Media** task. The Enable FTP Access to Mass Storage Media message window is displayed.
2. Click **Yes**, the Enable FTP Access to Removable Mass Storage Media window is displayed.
3. Specify the TCP/IP address or host name of the system processor that requires access to the Hardware Management Console for the mass storage media. The Enable FTP Access to Mass Storage Media message window is displayed.
4. Specify the user ID and password information from the **Load from Removable Media or Server** task.
5. Click **CLOSE** when you no longer need the FTP access and the installation is complete.

Use the online Help if you need additional information for enabling FTP access to mass storage media or see Appendix H, “Installing software from a mass storage device,” on page 249.

Fibre Channel Analyzer



Note: To view the errors on the fibre channel, using this task, you must enable the **Fibre channel analysis** option from the **Customize Console Services** task.

This task displays the errors on the fibre channels of attached Support Elements to assist in identifying link and control unit problems. The information is analyzed to detect the trends and thresholds and reports the results to you.

To view the information:

1. Open the **Fibre Channel Analyzer** task. The Fibre Channel Error Summary window is displayed. The error logs displayed contain information about the following:
 - System
 - PCHID
 - Source Link Address
 - Destination Link Address
 - CHPID
 - Channel Type.
2. Select one of the systems to view additional information. The Error Summary Output portion of the window displays this additional information.
3. Click **Cancel** when you are done reviewing the information.

Use the online Help to get additional information about the fibre channel analyzer.

Format Media



Note: You cannot perform this task remotely.

This task formats removable media (DVD-RAM, USB flash memory drive, or diskette (if one is available)).

Use this task to select the appropriate format type for the removable media.

- Change Management System Update Level
- Backup/Restore
- Service Data
- Upgrade Data
- Security Log
- Virtual RETAIN
- User-specified label.

To format a DVD-RAM, diskette (if one is available), or USB flash memory drive (see “USB flash memory drive” on page 10 for more information):

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**.
3. The Select Media Device window is displayed. Select the media you want to format, then click **OK**.
4. When the media is formatted, the Format Media Completed window is displayed.

Use the online Help if you need additional information for formatting removable media.

Hardware Management Console Settings



Notes:

- This task is available only when using the classic style user interface.
- If Customizable Data Replication is **Enabled** on this Hardware Management Console (using the **Configure Data Replication** task), the data 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” on page 86.

The **Hardware Management Console Settings** task contains a collection of the following settings-related tasks when using the classic style user interface. Otherwise, these individual tasks can be found under the **HMC Management** and **Service Management** nodes when using the tree style user interface:

Configure Data Replication

Enable or disable the ability of the Hardware Management Console to act as a server of customizable console data and to indicate whether the Hardware Management Console can accept customizable console data sent by another Hardware Management Console. See “Configure Data Replication” on page 86 for more information.

Customize API Settings

Enable or disable an SNMP agent, set up a community name file and event notification information. See “Customize API Settings” on page 90 for more information.

Customize Auto Answer Settings

Define the login name and password for point-to-point protocol (PPP) dial-up connection to the Hardware Management Console. See “Customize Auto Answer Settings” on page 90 for more information.

Customize Automatic Logon

Enable or disable the automatic logon feature. See “Customize Automatic Logon” on page 91 for more information.

Customize Console Services

Enable or disable remote operation, remote restart, LIC change, optical error analysis, CIM management interface, console messenger, fibre channel analysis. See “Customize Console Services” on page 93 for more information.

Customize Customer Information

Customize company information and account information. See “Customize Customer Information” on page 94 for more information.

Customize Modem Settings

Configures basic modem settings for remote support. See “Customize Modem Settings” on page 95 for more information.

Customize Network Settings

View and change network information which includes identifying your console, selecting a Local Area Network (LAN) adapter, specifying Domain Name Services (DNS), and specifying routing information for configuring the console network settings. See “Customize Network Settings” on page 95 for more information.

Customize Outbound Connectivity

Customize outbound connectivity for the Hardware Management Console to use remote service. See “Customize Outbound Connectivity” on page 97 for more information.

Customize Product Engineering Access

View or change authorization of IBM Product Engineering access to the Hardware Management Console. See “Customize Product Engineering Access” on page 99 for more information.

Customize Remote Service

Enable remote service requests, authorize automatic service call reporting. See “Customize Remote Service” on page 99 for more information.

Object Locking Settings

Control which managed objects are automatically locked and whether they are relocked after being used as target objects for a task. See “Object Locking Settings” on page 114 for more information.

To access the tasks under the Hardware Management Console using the classic user interface:

1. Open **Console Actions** from the **Views** area.
2. Open **Hardware Management Console Settings** from the **Console Actions Work Area**. The **Hardware Management Console Settings Work Area** is displayed.

Installation Complete Report



Note: You cannot perform this task remotely.

This task is used by service representatives to report installation information. This information is used by IBM to assess the success of the installation and make improvements in the installation processes. The information can be transmitted directly to IBM Service 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 IBM Service Support System.

Use the online Help to get additional information for sending installation information to IBM.

Logoff or Disconnect



Note: If you are using the tree style user interface this task is located on the right side of the task bar, click **Logoff** to access.

This task allows you to end the current user session and logs off the Hardware Management 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 Hardware Management Console application is running. If the Hardware Management 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 Hardware Management Console. Logging off the console does not affect the status of the CPC or images. After you log off or disconnect, the Welcome to the HMC 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.)

To log off the Hardware Management 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 Hardware Management Console.

To disconnect from the Hardware Management 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 Hardware Management Console with the intent of returning at a later time.

Use the online Help if you need additional information about logging off the Hardware Management Console or disconnecting from your session.

Manage Enterprise Directory Server Definitions



This task, used by an access administrator or a user ID that is assigned access administrator roles, creates new enterprise server (LDAP) definitions or edits and removes existing enterprise directory server definitions.

The Lightweight Directory Access Protocol (LDAP) support allows you the option to configure your Hardware Management 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.

The **User Profiles** task is used to choose which type of server authentication you prefer: **Local Server** or **LDAP Server**.

To add, edit, or remove an enterprise directory (LDAP) server:

1. Open the **Manage Enterprise Directory Server Definitions** task. The Manage Enterprise Directory Server Definitions window is displayed.
 - To add a server, click **Add...** The Add Enterprise Directory (LDAP) Server window is displayed. Provide the appropriate information, then click **OK**.
 - To edit a server, select a server then click **Edit...** The Edit Enterprise Directory (LDAP) Server window is displayed. Provide the appropriate information, then click **OK**.
 - To remove a server, select a server, then click **Remove**.
2. When you have completed the task, click **Close**.

Use the online Help if you need additional information for setting up an LDAP server.

Manage Print Screen Files



Note: If you access this task remotely you can only view or delete the print screen files that appear in the task window.

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**.

Use the online Help if you need additional information for capturing and managing the print screen files.

Manage Remote Connections



Note: The Hardware Management Console's call-home server service must be enabled for you to use this task.

This task allows you to view or manage remote connections. The Hardware Management Console manages remote connections automatically. It puts requests on a queue and processes them in the order in which they are received. However, this task allows you to manage the queue manually, if necessary. You can stop transmissions, move priority requests ahead of others, or delete requests.

To manage remote connections:

1. Open the **Manage Remote Connections** task. The Manage Remote Connections window is displayed.
2. This window lists active requests (being transmitted) and those that are waiting. You can select requests in the lists. You can display options by clicking **Options** on the menu bar. The options permit you to:
 - Prioritize a selected request (move it to the top of the queue)
 - Cancel selected requests
 - Cancel all active requests (those being transmitted)
 - Cancel all waiting requests
 - Hold the queue (puts queue on hold after completing current active request)
 - Release the queue
 - Close the window and exit.
3. Select **Options** (from the menu bar), **Exit** when you have completed the task.

Use the online Help if you need additional information for manually managing remote connections.

Manage Remote Support Requests



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 Hardware Management Consoles 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.

Use the online Help if you need additional information for manually managing remote connections.

Manage SSH Keys



This task allows you to install the public key for a host used for secure transfers. It associates a public key with a host address and allows a secure FTP connection from a Hardware Management Console FTP client to an FTP server location.

To manage SSH keys:

1. Open the **Manage SSH Keys** task. The Manage SSH Keys window is displayed.
2. Specify an IP address that you want associated with a secure host key, then click **Add**. This IP address and its corresponding key is displayed in the **Known Host Keys** table.
3. You can select an existing IP address from the table, then click **Delete** to remove it.
4. When you have completed this task, click **Close**.

Use the online Help to get additional information for managing SSH keys.

Manage Users Wizard



This task, used by an access administrator or a user ID that has access administrator roles, uses a wizard for creating and updating users and user roles, setting up user authentication, and establishing user settings.

When you are creating a new user, the user settings that are initially displayed when you are going through this task are the default settings that were set in the **Console Default User Settings** task. When a setting is changed in the **Console Default User Settings** task those new settings will now be the initial settings that are used if you create a new user with this task.

You can also use the individual tasks to set up this information:

- User Profiles
- Customize User Controls
- Password Profiles
- User Settings
- Manage Enterprise Directory Server Definitions

To use the wizard:

1. Open **Manage Users Wizard**. The Manage User Wizard window is displayed.
2. Proceed through each page of the wizard by providing appropriate information or selections, click **Next>** each time you have finished a page of the wizard. You can click **Back>**, however you could lose some of the information you have already provided.
3. When you have completed all the tasks (pages) in the wizard for creating a new user or updating an existing user, click **Finish**.

Manage Web Services API



This task allows you to view the web services API logs. You can also save the log file to your workstation or copy it to removable media (USB flash memory drive, DVD-RAM, or diskette).

To view or save the web services API log file:

1. Open the **Manage Web Service API** task. The Manage Web Services API Logs window is displayed.
2. You can make one of the following selections:
 - **View Web Services Log**, then click **OK**. The View Web Services Log window is displayed. When you are done viewing the log and ready to exit the task, click **Cancel**.
 - **Save Web Services Log**, then click **OK**. The Save File window is displayed. Select the link to save the file to your workstation, then click **OK** to proceed. The windows that follow allow you to indicate where you want to save the log file.

Use the online Help if you need additional information for viewing or saving the web services API log.

Monitor System Events



Notes:

- For this task, an SMTP email server must be accessible from the Hardware Management Console. (This is because all notifications from this task use email.)
- See “Monitor System Events” on page 192 when you are managing z/VM virtual machines from the Hardware Management Console.

This task allows you to create and manage event monitors. Event monitors listen for events from objects the Hardware Management Console manages. The types of events include:

- State changes
- Hardware messages
- Operating system messages
- Security log

- CPU Utilization
- Performance Index (PI)

When an event is received, the monitor tests it with user-defined time and text filters. If the event passes the tests, the monitor sends email to interested users. The **Monitor System Events** task lets you enable or disable monitors, display or change information about settings such as the SMTP port.

An example of an event monitor you can create is one that listens for hardware messages. You also use the **Monitor System Events** task for pager notification. (Paging services typically support email forwarding to pagers, so no special support for paging is provided.)

An event monitor has the following characteristics:

- Unique name on the Hardware Management Console
- Persistent
- Enabled or disabled without changing its other characteristics
- Listens to one or more managed objects
- Notifies users by email if an event is received from a managed object and it passes through all of the event monitor's filters
- Contains a regular expression filter that must match the event text for the monitor to notify users
- Limited by time filters, such as the following:
 - A set of days, for example, Monday through Friday
 - A range of times during the day, for example 8 a.m. through 4 p.m.
 - A range of dates, for example, 2/14/2005 to 2/16/2005.

To create or change an event monitor:

1. Open the **Monitor System Events** task. The Event Monitor Summary window is displayed.
2. From this window you can:
 - View or change **Settings** information:
 - SMTP server
 - SMTP port
 - Minimum time between emails.
 - Enable or disable **Monitors** information:
 - Name
 - Description
 - Enabled status.
 - To add, edit, or delete an event monitor, select it in the **Monitors** table and click **Add...**, **Edit...**, or **Delete**, respectively.
 - To test an event monitor for the specified SMTP server, click **Test...**
3. Click **OK** to exit the task.

Use the online Help if you need additional information about creating and managing event monitors.

Network Diagnostic Information



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 Hardware Management 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)
 - User Datagram Protocol (UDP)
 - Internet Protocol (IP) Tables
 - Native Connections
 - Test Support Element Communications (This tab is available only for user IDs with service or access administrator roles.)
3. Click **Cancel** when you are done viewing the information.

Use the online Help to get additional information on your console's network information.

Object Locking Settings



Notes:

- Because there are really many main user interfaces (one for each logged on user), the Hardware Management Console provides object locking capabilities for each user. This means that users have their own individual object locking settings, managed by using the **Object Locking Settings** task, and their own state information for locked objects. In other words, if you lock or unlock an object, it is not locked or unlocked respectively for other logged-on users.
- If you are using the classic style user interface, this task is found under the **Hardware Management Console Settings** console action.

This task allows you to control whether managed objects are automatically locked and whether they are relocked 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.

Use the online Help to get additional information for changing object locking settings. See also "Disruptive tasks" on page 6 for more information.

Offload Virtual RETAIN Data to Removable Media



Note: You cannot perform this task remotely.

Virtual RETAIN is a set of subdirectories that contain all the files that would have been transmitted to the IBM Service Support System (RETAIN) if a connection to IBM Service Support System were available. A subdirectory is dynamically created for each problem reported on a machine that was unable to send data to the IBM Service Support System.

To offload the data for a given problem within one of these subdirectories directly to removable media on the Hardware Management Console:

1. Open the **Offload Virtual RETAIN Data to Removable Media** task. The Virtual RETAIN Data Offload window is displayed.
2. Select the *problem number* of the subdirectory you want to offload from the list.
3. Insert a formatted removable media.
4. Click **OK**. The offload process takes several minutes to complete, depending on the size and quantity of the files to be transferred to removable media.

Use the online Help if you need additional information for offloading Virtual RETAIN data to a removable media.

Password Profiles



This task, used by an access administrator or a user ID that is assigned access administrator roles, creates, customizes, or verifies the password rules assigned to the system users. 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.

To set a password profile:

1. Open the **Password Profiles** task. The Password Profiles window is displayed.
2. Select a password rule or create your own and select properties for the password rule.
3. Click **OK** to complete the task or **Cancel** to exit the task

Use the online Help if you need additional information for creating a password profile.

Perform a Console Repair Action



Note: You cannot perform this task remotely.

This task should be the starting point for all Hardware Management Console repairs. You can either repair an open problem or report a repair of a non-detected problem.

To start a console repair action:

1. Open the **Perform a Console Repair Action** task. The Perform a Console Repair Action window is displayed.
 - To start a repair or continue a repair of a previously reported problem, select **Repair an open problem**.

- To report to IBM about repairing a problem that was not detected or reported by Problem Analysis, select **Report a repair of a non-detected problem**.
2. Click **OK** to start the repair.

Use the online Help if you need additional information on starting a repair action.

Reassign Hardware Management Console



Note: You cannot perform this task remotely.

This task allows you to reassociate the Hardware Management Console with a different CPC. CD-ROM data must be obtained prior to starting this task from the **S/390 Special Request** website. To access the data, enter the following web address:

<http://gemserv6.pok.ibm.com/s390req>

The S/390® Special Requests home page is displayed. Click on the **Account Team** *initiate a request* option. From **Request Type** list, click the **HMC Move** option, fill in the rest of the information that is required on that window, then click **Continue**. After you have your CD-ROM with the required information, continue with this task.

Use the online Help if you need additional information for reassigning the Hardware Management Console.

Rebuild Vital Product Data



Note: Do not rebuild the Vital Product Data unless you have been directed by Product Engineering.

This task forces a rebuild of the Vital Product Data on the Hardware Management Console. Before a rebuild is done, the current version will be saved.

To rebuild the vital product data:

1. Open the **Rebuild Vital Product Data** task. The Rebuild Vital Product Data window is displayed.
2. Click **OK** to continue with this task.
3. After the vital product data is rebuilt, a message displays that the rebuild was successful.
4. Click **OK** to complete the task.

Note: If a failure occurs, an error will be logged in the default system log.

Use the online Help if you need additional information.

Remote Hardware Management Console



Notes:

- You cannot perform this task remotely.
- You can only establish a remote session to another Hardware Management Console if the following conditions are met:
 - The Hardware Management Consoles are in the same domain. To verify the domain, use the **Domain Security** task.
 - Remote operation is enabled on the remote Hardware Management Console. To enable remote operation, use the **Customize Console Services** task.

This task allows the local Hardware Management Console user to open a browser session to another Hardware Management Console.

To establish a remote session:

1. Open the **Remote Hardware Management Console** task. The Remote Hardware Management Console Addressing Information window is displayed.
2. Specify the IPv4 or IPv6 TCP/IP address or host name of the remote Hardware Management Console you want to contact.
3. Click **OK** to complete the task or **Cancel** to exit.

Use the online Help if you need additional information about contacting another Hardware Management Console.

Report a Problem



This task reports problems that occurred on your Hardware Management Console to the IBM Service Support System (for example, the mouse does not work) or lets you test problem reporting.

Submitting a problem is dependent upon whether you have enabled authorized automatic service call reporting. You can do this by using the **Customize Remote Service** task and selecting **Authorize automatic service call reporting**. If it is enabled and you have a call-home server available, it will automatically send the problem to the IBM Service Support System.

If **Authorized automatic service call report** is not enabled, the problem will be logged in the Hardware Messages. You can subsequently send the problem to the IBM Service Support System by selecting the Hardware Management Console, access **Hardware Messages**, select the messages you want information on, click **Details...** in the Hardware Messages window. You will get the Problem Analysis window where you will click **Request Service....**

To report a problem on your Hardware Management Console:

1. Open the **Report a Problem** task. The Report a Problem window is displayed.
2. Select a problem type then enter a brief description of your problem in the **Problem Description** input field.
3. 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**.

Use the online Help if you need additional information for reporting a problem or testing if problem reporting works.

Restore Legacy HMC Data



This task restores customizable Hardware Management Console (HMC) data from the backup restore DVD-RAM of a Hardware Management Console Version 1.8.2 or earlier.

To restore the data:

1. Open the **Restore Legacy HMC Data** task. The Restore Customizable Data window is displayed.
2. Insert the backup restore DVD-RAM into the DVD-RAM drive.
3. Select the appropriate restore option, then click **OK** to restore the data.

Use the online Help if you need additional information for restoring legacy Hardware Management Console data.

Save Upgrade Data



This task saves all of the customizable data for your Hardware Management Console to the hard drive or USB flash memory drive (see “USB flash memory drive” on page 10 for more information) before performing an Engineering Change (EC) upgrade.

To save the Hardware Management Console customized data to the hard drive:

1. Open the **Save Upgrade Data** task. The Save Upgrade Data window is displayed.
2. Select **Save to 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.

Additionally, you can save customized data from an existing Hardware Management Console with this task. The following procedure will copy customized data from a Hardware Management Console at Licensed Internal Code Version 1.8.2 to a Hardware Management Console at Licensed Internal Code Version 2.9.0 or later. Some data is not transferable using this procedure and must be moved manually.

1. From the **Save Upgrade Data** window, select **Save to hard drive**.
2. Insert the **HWMCA - Save/Restore Customizable Console Data** diskette, P/N 41V1443, into the diskette drive of the Hardware Management Console at Licensed Internal Code Version 1.8.2.
3. Log off and shutdown the Hardware Management Console.
4. When shutdown completes, reboot the Hardware Management Console. (The diskette is bootable and it will give you a selection panel.)
5. Select **Save Hardware Master Console customizable data**. This is option F1.

6. A successful completion message will be displayed when complete. Remove the diskette from the Hardware Management Console at Licensed Internal Code Version 1.8.2.

Finally, the following procedure restores Customizable Data on the Hardware Console at Licensed Internal Code Version 2.9.0 or later.

1. Power off the Hardware Management Console at Licensed Internal Code Version 2.9.0 or later.
2. Install the **HWMCA - Save/Restore Customizable Console Data** diskette into the diskette drive of the Hardware Management Console at Licensed Internal Code Version 2.9.0 or later.
3. Power on the Hardware Management Console. (The diskette is bootable and will give you a selection panel.)
4. Select **Restore Hardware Master Console customizable configuration data**. This is option F8.
5. A successful completion message will be displayed when complete.
6. Remove the diskette from the diskette drive.
7. Reboot the Hardware Management Console at Licensed Internal Code Version 2.9.0 or later. The system will restore the data on the reboot.

Use the online Help if you need additional information for saving upgrade data.

Save/Restore Customizable Console Data



Notes:

- You cannot perform this task remotely.
- If **Customizable Data Replication** is *Enabled* on this Hardware Management Console (using the **Configure Data Replication** task), the data 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” on page 86.
- There is a **Save/Restore Customizable Console Data** DVD-RAM available for saving customized data from an existing Hardware Management Console, see “Save Upgrade Data” on page 118.

This task, used by an access administrator or a user ID that is assigned access administrator roles, enables you to save the following customizable Hardware Management Console data:

Associated Activation Profiles

Any activation profiles associated with CPC and CPC image objects.

Remote Service Data

Whether or not you have enabled remote service to allow automatic console connections to the IBM Service Support System.

Acceptable Status Settings

Any status settings that are considered acceptable for all types of managed objects.

Monitor System Events Data

Data for the **Monitor System Events** task including:

- The SMTP server and port settings
- The setting for the minimum time between emails
- The event monitors.

Outbound Connectivity Data

Information for dialing out, such as whether to enable the local system as a call-home server, or whether to allow dialing to use the local modem, the dial prefix, and phone numbers.

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.

Modem Configuration Data

Dial type (tone or pulse) and other settings such as whether to wait for a dial tone.

Customer Information Data

Data for a CPC or a group of CPCs which includes administrator, system, and account information about the system being installed.

Domain Security Data

Security definitions (domain name and password) for your Hardware Management Consoles and CPC Support Elements in your processor complex.

Object Locking Data

Whether to automatically lock all managed objects or whether to relock after a task runs.

Group Data

All user-defined group definitions.

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 a device or click **Restore** to restore data from a device. In either case, the Select Media Device window is displayed.
5. Select the device you want to save the data to or restore the data from. Your choices could be a DVD-RAM, USB flash memory drive, or diskette (if one is available). See “USB flash memory drive” on page 10 for more information.
6. Click **OK** to proceed with the task, click **Refresh** to update the device list, or click **Cancel** to go back to the previous window without saving or restoring the data.

After saving this data, you can restore it to the same Hardware Management Console or to another Hardware Management Console.

Use the online Help if you need additional information about saving or restoring customizable console data.

Shutdown or Restart



This task enables you to restart the application, restart the console, or power-off the console if you are accessing the Hardware Management Console locally. If you are accessing the Hardware Management Console remotely you can only restart the console if the **Remote restart** service is enabled from the **Customize Console Services** task.

To shut down or restart the application or console:

1. Open the **Shutdown or Restart** task. The Shutdown or Restart window is displayed.
2. You can select one of the following:

- Restart console
 - Power-off console
3. Click **OK** to perform the selected action or click **Cancel** to return to the Hardware Management 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.

Use the online Help if you need additional information about shutting down or restarting the Hardware Management Console.

Single Step Console Internal Code



Note: You can perform this task remotely only if a USB flash memory drive (formatted with volume label of **ACTBKP**) is in the Hardware Management Console. (See “USB flash memory drive” on page 10 for more information.)

This task allows you to retrieve and apply, apply only, or remove licensed internal code on the Hardware Management Console. For information on retrieving and applying, applying only, or removing licensed internal code to an object, see “Single Step Internal Code Changes” on page 166.

The purpose of this task is to:

- Determine whether to only apply internal code changes or to retrieve and apply internal code changes.
- Verify the system environment.
- Perform a Backup Critical Console Data function.
- Accept all previously activated internal code changes (optional).
- Retrieve internal code changes from the IBM Service Support System, if retrieve and apply is the selected operation.
- Connect to the IBM Service Support System and verify the current status of all downloaded internal code changes.
- Install and activate the internal code changes.

To retrieve and apply, apply only, or remove licensed internal code on the Hardware Management Console:

1. Open the **Single Step Console Internal Code** task. The Single Step Console Internal Code window is displayed.
2. Select the Single Step Internal Code Change option you want to perform, then click **OK**. (If you do not want to make the previously installed internal code changes permanent, select **Accept execution phase to be excluded**.)
3. Follow the instructions on the subsequent windows to complete the task.

Use the online Help to get additional information on working with an internal code change.

Tip of the Day



This task allows you to view information about using the Hardware Management Console. A different fact or tip is displayed each time you log on.

To control the tip of the day message:

1. Open the **Tip of the Day** task. The Tip of the Day window is displayed.
2. You can select the following options from this window:
 - Select **Show tips each time you log on** to display a tip each time you log on to the Hardware Management Console.
 - Click **Previous Tip** or **Next Tip** to scroll through the information.

Note: You can also control the display of the tips by using the **User Settings** task. From the User Settings window, select the **Controls** tab and select or deselect **Show tips each time you log on**.

3. Click **Close** when you have completed this task.

Transmit Console Service Data



This task provides the ability to send information that is stored on the Hardware Management Console hard disk that can be used for problem determination.

The data may be *traces*, *logs*, or *dumps* and the destination for the data may be the IBM Service Support System, a diskette (if one is available), USB flash memory drive, or a DVD-RAM. (See “USB flash memory drive” on page 10 for more information.)

Before you can send information to the IBM Service Support System, Phone Server and Remote Service must be *enabled*. To enable remote service, see “Customize Console Services” on page 93. To enable telephone server, see “Customize Outbound Connectivity” on page 97.

To transmit console service data:

1. Open the **Transmit Console Service Data** task. The Transmit Service Data to IBM window is displayed.
2. Select the type of data you want transmitted along with any additional information, including the destination.
3. Click **Send** to send the information to the selected destination or **Cancel** to exit the task without sending any information.

Use the online Help for additional information about getting selected service data from the Hardware Management Console hard disk and sending it to IBM.

Transmit Vital Product Data



This task collects Vital Product Data (VPD) from the Hardware Management Console and either transmits the data to the IBM Service Support System or stores the information on diskette (if one is available), USB flash memory drive, or the Hardware Management Console hard disk. (See “USB flash memory drive” on page 10 for more information.)

Note: To transmit the data to the IBM Service Support System, the Hardware Management Console must be enabled for using the Remote Support Facility (RSF). If the Hardware Management Console is not equipped and enabled for using the RSF, select **Diskette** to copy the VPD to a diskette to mail to IBM.

To transmit vital product data:

1. Open the **Transmit Vital Product Data** task. The Transmit Vital Product Data to IBM window is displayed.
2. Select one of the VPD destinations.
3. Click **OK** to continue with the task, or **Cancel** to end the task.

Use the online Help if you need additional information for transmitting VPD data for the Hardware Management Console.

User Patterns



Note: If Customizable Data Replication is *Enabled* on this Hardware Management Console (using the **Configure Data Replication** task), the data 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” on page 86.

The “User Templates” on page 128 task and **User Patterns** task control adding or removing console users through your own corporate security environment, such as an LDAP server. A user ID pattern encapsulates all the information needed to create a temporary user definition.

This task, used by an access administrator or a user ID that is assigned access administrator roles, defines:

- The pattern to be used to try and match unknown user IDs not defined to the Hardware Management Console to user IDs in a specified LDAP server
- A defined template to be used for matching user IDs
- An LDAP server definition to validate the user ID when processing a logon for users that match the pattern
- The retention time (in days) for modified user setting information
- Optionally, LDAP attributes and LDAP server definition used to determine the user template to be used or domains where the pattern is valid

Note: LDAP server used for authentication can be different from the one used to specify the template and domain names.

To customize a user pattern:

1. Open the **User Patterns** task. The User Pattern window is displayed.
2. Select the type of string pattern you want to customize.
 - If you are creating a string pattern, select **Add...** from the menu bar. The Add Pattern window is displayed.
 - If the string pattern name exists in the window, select the string pattern name from the list and then select **Modify...** from the menu bar. The Modify Pattern window is displayed.
3. Complete or change the fields in the window, click **OK** when you are done.

Use the online Help for more information for customizing the user patterns.

User Profiles



Note: If Customizable Data Replication is *Enabled* on this Hardware Management Console (using the **Configure Data Replication** task), the data 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” on page 86.

This task, used by an access administrator or a user ID that is assigned access administrator roles, manages your system users that log on to the Hardware Management Console. A user profile is a combination of a user ID, permissions, authentication mode, and a text description. Permissions represent the authority levels assigned to the user profile for the objects the user has permission to access.

The user ID and password are used to verify a user's authorization to log on to the Hardware Management Console. The user ID can be 4 - 320 characters in length and can be a combination of uppercase and lowercase letters (A-Z, a-z), numbers (0-9), and special characters (@ \ < + : # ' = " & * () ; - / , % _ > . ?). The password is determined by the password rule that is chosen for the user ID. The default choices are *basic*, *strict*, and *standard*, however, other rules may also be available if they were defined in the **Password Profiles** 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 login, and whether you can log on to the Hardware Management Console.

Use this task to choose the type of password authentication you want to assign to a user ID. If you choose the **Local Authentication**, then the password authentication is performed by using the Hardware Management Console. If you choose the **LDAP Server**, then the password authentication is delegated to an enterprise director (LDAP) server. You use the **Manage Enterprise Directory Server Definitions** task to define the LDAP server.

The user profile includes managed resource roles and task roles that are assigned to the user. The *managed resource roles* assign permissions for a managed object or group of objects and the *task roles* define the access level for a user to perform on a managed object or group of objects. You can choose from a list of available default managed resource roles, task roles, or customized roles created by using the **Customize User Controls** task.

See Appendix A, “Tasks and default user IDs,” on page 203 for a listing of all the Hardware Management Console tasks and the predefined default user IDs that can perform each task.

To customize a user profile:

1. Open the **User Profiles** task. The User Profiles window is displayed.
2. Select the type of user ID you want to customize.
 - If you are creating a user ID, point to **User** on the menu bar and when its menu is displayed, click **Add....** The Add User window is displayed.

Note: When you create a user ID, the new user ID is set to use the default user interface style. If you create a user ID that is copied from an existing user ID, the new user ID gets the user interface style of the user ID it is being copied from.

- If the user ID exists in the window, select the user ID from the list, and then point to **User** on the menu bar and when its menu is displayed, click **Modify....** The Modify User window is displayed.
3. Complete or change the fields in the window, click **OK** when you are done.

Use this task to give access to specific user IDs for the Hardware Management Console web server. The web server is a remote capability that allows you to monitor and control defined CPCs, CPC images, or groups from a remote site to a local Hardware Management Console through a web browser.

To give access to the web server from the User Profiles window:

1. Select the type of user ID you want to give web server access to.
 - If the user ID you want to give access to exists in the window, select the user ID from the list, and then point to **User** on the menu bar and when its menu is displayed, click **Modify....** The Modify User window is displayed.
 - If you are creating a user ID, point to **User** on the menu bar and when its menu is displayed, click **Add....** The Add User window is displayed.
2. Click **User Properties....**, the User Properties window is displayed.
3. Select **Allow remote access via the web** (a check mark is displayed) and then click **OK**. This user ID now has access to the web server.

Note: Repeat steps 1 through 3 for each additional user ID you want to give access to the web server.

| Use this task to give specific user IDs permission to use an Application Programming Interface (API).

| To give access to the interfaces from the User Profiles window:

- | 1. Select the type of user ID you want to give API access to.
 - | • If the user ID you want to give access to exists in the window, select the user ID from the list, and then point to **User** on the menu bar and when its menu is displayed, click **Modify....** The Modify User window is displayed.
 - | • If you are creating a user ID, point to **User** on the menu bar and when its menu is displayed, click **Add....** The Add User window is displayed.
- | 2. Click **User Properties....**, the User Properties window is displayed.
- | 3. Select **Allow access to management interfaces** (a check mark is displayed) and then click **OK**. This user ID now has access to the interfaces.

| **Note:** Repeat steps 1 through 3 for each additional user ID you want to give access to the interfaces.

Use this task to request text input on the Disruptive Task Confirmation window or have a specific user ID password specified before you proceed with a task that causes disruptive actions. To set these options from the User Profiles window:

1. Select the user ID, point to **User** on the menu bar, then click **Modify....** The Modify User window is displayed.
2. Click **User Properties....**, the User Properties window is displayed.
3. Select **Require password for disruptive actions** (a check mark is displayed), then click **OK**. When this user ID tries to execute a task that causes disruptive actions, the Disruptive Task Confirmation window displays a password input field. The user must specify the password before proceeding with the task. (See “Disruptive tasks” on page 6 for more information.)
4. Select **Require text input for disruptive actions** (a check mark is displayed), then click **OK**. When this user ID tries to execute a task that causes disruptive actions, the Disruptive Task Confirmation window displays a Confirmation Text input area for each affected object. Specify the operating system name, if available, otherwise the system name must be provided to proceed. (See “Disruptive tasks” on page 6 for more information.)

Use the online Help for more information for customizing the user profiles.

User Settings



Notes:

- If Customizable Data Replication is *Enabled* on this Hardware Management Console (using the **Configure Data Replication** task), the data 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” on page 86.
- Only a user ID assigned access administrator roles sets the defaults of the Hardware Management Console settings by using the **Console Default User Settings** task.
- Because there are many main users interfaces (one for each logged on user), the Hardware Management Console provides each user the ability to change settings, such as color or patterns and confirmation settings. In other words, if you change confirmation settings or colors and patterns, this does not cause that same change for other logged-on users.

This task enables you to customize settings that control how the Hardware Management Console operates.

You can select the user interface style that you want to work with (tree or classic) if the default has been set to allow you to change the interface. (This option is set by the access administrator from the **Console Default User Settings** task.) You also are able to choose whether you want hover help, single object selection, show tips, or choose when to display or not display confirmation windows.

Tree style user interface

If you are using the tree style user interface, use the following steps to define the user settings:

1. Open the **User Settings** task. The User Settings window is displayed.
2. Proceed through the following tabs to customize your Hardware Management Console workplace:

Tree Style

Use this tab to select the appearance of the tree style user interface Hardware Management Console workplace. This tab is available only for the tree style interface. The following options are available:

- Banner
- Tasks pad
- Navigation icons
- Work pane icons

For example, if you want to display the banner when you are using the tree interface, you need to:

- a. Open the **User Settings** task by clicking on the user ID on the task bar or click on the **HMC Management** node in the navigation pane and click on **User Settings** in the work pane. The User Settings window is displayed.
- b. Select the **Tree Style** tab. Select Banner if you want it to appear on the workplace (a check mark is displayed).
- c. Click **Apply** to have the changes take affect, click **OK** to close the window.
- d. The banner is displayed as part of the workplace window.

Confirmations

Use this tab to customize preferences for confirmation windows that are used for a subset of tasks. The settings options you can select from include:

- Enabled with object list
- Enabled without object list
- Do not show confirmations

You can also select **Use 'No' as the default action** indicating that the default action for the confirmation window is to cancel the task. The **No** button is preselected on the confirmation window so you can press Enter to cancel the task.

Controls

Use this tab to control the following functions:

- Single object selection
- Show tips each time you logon
- Accept Console Messenger messages (This is available only if the **Console messenger** facility is enabled from the **Customize Console Services** task.)
- Bring Chat Window to foreground on new messages (This is available only if the **Console messenger** facility is enabled from the **Customize Console Services** task.)

UI Style

Use this tab to select the user interface style you prefer to work with. You can choose from the following:

- Tree style (see Chapter 3, “Using the tree style user interface,” on page 15 for more information)
- Classic style (see Chapter 4, “Using the classic style user interface,” on page 47 for more information)

3. Click **Apply** to save the settings currently displayed or changed, or

Click **Reset** to discard any changes you made to the settings after you opened this task and redisplay the current settings for this user ID, or

Click **Defaults** to discard any changes you made to the settings at any time and redisplay the original default settings for this user ID.

4. Click **OK** to save the settings and end the task or click **Cancel** to exit this task without making any changes.

Use the online Help to get additional information for customizing user settings for the Hardware Management Console workplace.

Classic style user interface

If you are using the classic style user interface, use the following steps to define the user settings:

1. Open the **User Settings** task. The User Settings window is displayed.
2. Proceed through the following tabs to customize your Hardware Management Console workplace:

Confirmations

Use this tab to customize preferences for confirmation windows that are used for a subset of tasks as described above for the tree style user interface.

Colors and Patterns

Use this tab to set color (or patterns) for indicating exceptions on the Hardware Management Console workplace. This tab is available only for the classic style user interface. You can adjust color settings for the following situations:

- Modify the default colors (or use gray patterns instead of color) that indicate processor cluster status changes.
- Associate a color or pattern with any of the status values that you indicate as unacceptable, thereby allowing you to distinguish between types of exceptions.

- Change the background color of the Views area for an exception or nonexception situation and change the color associated with pending messages. See “Monitoring your hardware” on page 55 for more information about status and exception conditions.

Controls

Use this tab to control the following functions:

- Show hover help (This option is available only for the classic style user interface.)
- Single object selection
- Show tips each time you logon
- Accept Console Messenger messages (This is available only if the **Console messenger** facility is enabled from the **Customize Console Services** task.)
- Bring Chat Window to foreground on new messages (This is available only if the **Console messenger** facility is enabled from the **Customize Console Services** task.)

Classic Style

Use this tab to change the appearance for the classic style user interface. You can choose options from the following areas of the task window:

- **Console Actions Layout Style** - allows you to display the console actions in a classic style user interface layout (default), a list format, or arranged in predefined groups.
- **Console Actions Sort Order** - allows you to display the tasks alphabetically or in the original classic style user interface order (default).
- **Show or Hide Areas** - allows you to hide areas of the interface to display more objects in another area.

Note: You can also change the classic style settings for the console actions by opening the pop-up menu from the work area. Right-click on an empty area of the work area, the pop-up menu is displayed. Select the **Style Settings** option and then choose the format you want to change for the console actions. Use the help information from the **User Settings** task for more information on the formatting choices.

UI Style

Use this tab to select the user interface style you prefer to work with. You can choose from the following:

- Tree style (see Chapter 3, “Using the tree style user interface,” on page 15 for more information)
- Classic style (see Chapter 4, “Using the classic style user interface,” on page 47 for more information)

3. Click **Apply** to save the settings currently displayed or changed, or

Click **Reset** to discard any changes you made to the settings after you opened this task and redisplay the current settings for this user ID, or

Click **Defaults** to discard any changes you made to the settings at any time and redisplay the original default settings for this user ID.

4. Click **OK** to save the settings and end the task or click **Cancel** to exit this task without making any changes.

Use the online Help to get additional information for customizing user settings for the Hardware Management Console workplace.

User Templates



Note: If Customizable Data Replication is *Enabled* on this Hardware Management Console (using the **Configure Data Replication** task), the data 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” on page 86.

The **User Templates** task and “User Patterns” on page 123 task control adding or removing console users through your own corporate security environment, such as an LDAP server.

This task, used by an access administrator or a user ID that is assigned access administrator roles, manages your system users, restricted to LDAP authentication, that log on to the Hardware Management Console. The user ID can be 4 - 320 characters in length and can be a combination of uppercase and lowercase letters (A-Z, a-z), numbers (0-9), and special characters (@ \ < + : # ' = " & * () ; - / , % _ > . ?).

The **LDAP Server** authentication is delegated to an enterprise director (LDAP) server. You use the **Manage Enterprise Directory Server Definitions** task to define the LDAP server.

The user template includes managed resource roles and task roles that are assigned to the user. The *managed resource roles* assign permissions for a managed object or group of objects and the *task roles* define the access level for a user to perform on a managed object or group of objects. You can choose from a list of available default managed resource roles, task roles, or customized roles created by using the **Customize User Controls** task.

See Appendix A, “Tasks and default user IDs,” on page 203 for a listing of all the Hardware Management Console tasks and the predefined default user IDs that can perform each task.

To customize a user template:

1. Open the **User Template** task. The User Templates window is displayed.
2. Select the type of template you want to customize.
 - If you are creating a template name, select **Add...** from the menu bar. The Add Template window is displayed.
 - If the template name exists in the window, select the template name from the list and then select **Modify...** from the menu bar. The Modify Template window is displayed.
3. Complete or change the fields in the window, click **OK** when you are done.

This task also allows you to give access to particular user IDs for the Hardware Management Console web server. The web server is a remote capability that allows you to monitor and control defined CPCs, CPC images, or groups from a remote site to a local Hardware Management Console through a web browser.

To give access to the web server from the User Templates window:

1. Select the type of template name you want to give web server access to.
 - If you are creating a template name, select **Add...** from the menu bar. The Add Template window is displayed.
 - If the template name exists in the window, select the template name from the list and then select **Modify...** from the menu bar. The Modify Pattern window is displayed.
2. Click **User Properties...**, the User Properties window is displayed.
3. Select **Allow remote access via the web** (a check mark is displayed) and then click **OK**. This user ID now has access to the web server.

Note: Repeat steps 1 through 3 for each additional user ID you want to give access to the web server.

Use the online Help for more information for customizing the user template.

Users and Tasks



This task displays a list of the tasks that are running and the users that are currently logged on to the Hardware Management Console.

To work with the users and tasks:

1. Open the **User and Tasks** task. The Users and Tasks window is displayed.
2. 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.
3. 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**.
 4. When you have completed the task, click **Close**.

Use the online Help to get additional information about the tasks that are running and the users currently logged on to the Hardware Management Console.

View Console Events



This task enables you to view a record of system events occurring on the Hardware Management 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**.

Use the online Help to get additional information about reviewing the console events and using the filtering options for the console events listed.

View Console Information



This task displays information about the Hardware Management Console and its licensed internal code. It also lists the engineering change (EC) number and state levels of each set of licensed internal code associated with the Hardware Management Console.

Licensed internal code controls many of the operations available on the Hardware Management Console. Internal code changes may provide new operations, or correct or improve existing operations.

IBM Product Engineering assigns the EC number to a set of licensed internal code. The number identifies 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 the console information:

1. Open the **View Console Information** task. The View Console Information window is displayed.
2. Select a licensed internal code from the list.
3. Click **EC Details...** to view the additional information about internal code state levels.
4. Click **OK** when you are done viewing the information.

Use the online Help to get additional information on viewing the Hardware Management Console and its licensed internal code information.

View Console Service History



This task displays the service history log for the Hardware Management Console. The service history is a record of problems occurring on the Hardware Management Console. Service history information is recorded by *Problem Analysis* that starts automatically and identifies the source of a Hardware Management Console problem. Service history entries are displayed with the most recent entry at the top of the record.

To view the console service history:

1. Open the **View Console Service History** task. The View Console Service History window is displayed.
2. A table is displayed that lists the problems. Select a problem, then use the options from the menu bar for additional information or sorting preferences.
3. Click **View**, **Exit** from the menu bar when you have completed this task.

Use the online Help to get additional information about reviewing the service history.

View Console Tasks Performed



This task allows the IBM service representative 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 Licenses



This task allows you to view the Licensed Internal Code (LIC) that you have agreed to for this Hardware Management Console.

To view the licenses:

1. Open the **View Licenses** task. The View Licenses window is displayed.
2. 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.

3. Click **OK** when you are done viewing this information.

View PMV Records



This task allows you to obtain the Problem Management Viewable (PMV) records issued to the IBM Service Support System for the Hardware Management Console. These problems are typically sent to the IBM Service Support System where errors are not recorded by the console. You are able to view and edit the PMV records on the console and you have the ability for an interactive dialog with an IBM service representative. A PMV record is initially created from the **Report a Problem** task specifying a problem type of **Type V Viewable PMH(PMV)**.

To view a PMV record:

1. Open the **View PMV Records** task. The View PMV Records window is displayed.
2. Click **Yes** to retrieve a list of the most recent records, otherwise click **No** to get a list of records without the latest updates. The View PMV Records message window is displayed. It indicates the PMV records that are being retrieved from the IBM Service Support System. This process can take a long time. You can click **Cancel** to stop the process and exit the task at any time.
3. When the records have been retrieved, the View PMV Records window displays a listing of the PMV records and corresponding machine.
4. Select a PMV record to view, click **View PMV**. A message is displayed indicating the retrieval of the PMV record. The View PMV Records window is displayed. From this window the following options are available:
 - To add a comment to the PMV record, click **Add Comment**. The View PMV Records window is displayed with a text input area. Provide a comment in the text input area and click **Add Comment**.
 - To refresh the details of the PMV record, click **Refresh PMV**. The PMV record displays the most current information.
 - To supply a screen capture of the problem in the PMV record, click **Add Attachment**. The View PMV Records window is displayed with the available screen captures you created using the **Manage Print Screen** task. Select one or more files and click **Upload Image**.
 - To view existing screen captures (files) available for download, click **View Available Attachments**. The View PMV window displays a list of attachments that can be downloaded for the PVM record. Select one or more attachments you want to download then click **Download Attachment**.
 - To view attachments on the PVM record, click **View Downloaded Attachments**. The View PMV Records window displays the screen captures you uploaded to the PVM record. To view an image, select one then click **View Image**.
5. To stop processing an action on a PVM record or to exit the task, click **Cancel** at any time.

Use the online Help if you need additional information for viewing PMV records.

View Security Logs



This task allows you to view the security events logged for the Hardware Management Console or a server (CPC). 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. From the menu bar you have the following options for viewing information:
 - To open security logs, click **File**, then one of the following options:
 - To open an archived security log on a mass readable media device (CD-ROM, DVD-RAM, or USB flash memory drive whose capacity is 1 GB or greater), select **Open Security Log, New**. See “USB flash memory drive” on page 10 for more information.
 - To open the Hardware Management Console's default security log, select **Open Security Log, Default**.
 - To close the window and end the task, select **Exit**.
 - To search the security log that is currently open, click **Search**, then one of the following options:
 - To search events by the time and date they occurred, select **By Date**.
 - To search for an event by its description, select **By Event**.
 - To search for events by a certain group, select **By Category**.
 - To view or alter the security log options, click **Options**, then one of the following options:
 - To enable the creation of a hardware message when the security log is approaching the maximum size, select **Create hardware message when approaching maximum, On**.
 - To disable the creation of a hardware message when the security log is approaching the maximum size, select **Create hardware message when approaching maximum, Off**.
 - To enable the creation of a security log event when the underlying network firewall denies a network connection, select **Log security event for network denial events, On**.
 - To disable the creation of a security log event when the underlying network firewall denies a network connection, select **Log security event for network denial events, Off**.
 - To display help for the current window, click **Help**.
3. When you are done viewing the security log and ready to exit the task, click **File, Exit**.

Use the online Help if you need additional information for viewing a security log.

What's New



This task is a wizard that describes new features for this version of the Hardware Management Console.

To view this information:

1. Open the **What's New** task. The What's New window is displayed. The left portion of the window lists the new features.
2. Select a feature for more detailed information about the enhancement. This information is displayed in the right portion of the window. You can also click **Next >** or **< Back** to proceed forward or backward through the enhancements.

Level 01a

3. Click **Finish** or **Cancel** to return to the Hardware Management Console workplace.

Chapter 6. Server tasks

This chapter describes the tasks used by the selected CPCs (servers).

To open these tasks using the classic style user interface, see “Task list” on page 76 or if you are using the tree style user interface, see “Opening tasks for the system” on page 21.

Note: If you cannot access these tasks, contact your Access Administrator. You can also refer to Table 3 on page 205 for a list of the server (CPC) tasks and the corresponding predefined user IDs that can perform these tasks.

The following groups of tasks are represented in the *Task List Work Area* for the classic interface and in the tasks pad, drop-down menu, or context menu for the tree interface.

- Daily
- Recovery
- Service
- Change Management
- Remote Customization
- Operational Customization
- Object Definition
- Configuration
- Energy Management
- Monitor
- z/VM Virtual Machine Management (is displayed if one or more CPC images are running z/VM V5.3 or later)

Daily



Daily contains the tasks for operating CPCs and CPC images.

The following tasks are represented in the *Daily* task group:

- Activate
- Deactivate
- Grouping
- Hardware Messages
- Operating System Messages
- Reset Normal

Note: The **Activity** task is accessed from the **Monitors Dashboard** task by selecting **Open Activity** from the menu bar.

Activate



Notes:

- Activate is considered a disruptive task. If the object is locked, you must unlock it before continuing. For more information about disruptive tasks, see “Disruptive tasks” on page 6.
- See “Activate” on page 194 when you are managing z/VM virtual machines from the Hardware Management Console.

This task controls starting up the system including power-on reset, partition activation, and initial program load of your operating system software. Activate is your primary function for CPC or CPC image start up. Activate senses the status of the object, then performs only those actions necessary to get the object to an operational state. For example, if the CPC is already in the power-on reset complete state, Activate skips the power-on reset step and proceeds with the load of the operating system.

If the CPC allows activation to include a power-on and the CPC is powered-off, Activate powers it on from the Hardware Management Console.

The Activate function uses profiles, which contain the parameters needed to put the system in an operational state. The profiles are stored in each CPC Support Element. A set of default activation profiles are shipped with the CPC. The values contained in these profiles might not be correct for your environment. See “About activation profiles” on page 8 for a description of activation profiles. See “Customize/Delete Activation Profiles” on page 174 for information about creating and modifying activation profiles.

To start activation:

1. Select one or more CPCs or CPC images.
2. Open the **Activate** task.

Note: If one or more of the selected CPCs have associated secondary objects (for example, an image or coupling facility image), a Secondary Object Notification for Disruptive Task message window is

displayed with a list of the active secondary objects. Review the list before proceeding. If you click **Yes** to proceed, the Activate Task Confirmation window is displayed. Review the confirmation text to decide whether to proceed with the task.

3. If you want to review the profile that is used for activation, click **View Activation Profile**; the View Activation Profiles window is displayed, showing the values that are set.
4. If you want to continue this task, click **Yes**. If you want to end the task, click **No**. If you click **Yes**, the Activate Progress window is displayed indicating the progress of the activation and the outcome.
5. 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.

Deactivate



Notes:

- Deactivate is considered a disruptive task. If the object is locked, you must unlock it before continuing. For more information about disruptive tasks, see “Disruptive tasks” on page 6.
- See “Deactivate” on page 195 when you are managing z/VM virtual machines from the Hardware Management Console.

This task stops the operating system, deallocates resources, and clears associated hardware for all selected CPCs or CPC images. In addition, if a CPC or a CPC image that represents a non-LPAR system is selected, the deactivate task will perform a power off.

To start deactivation:

1. Select one or more CPCs or CPC images.
2. Open the **Deactivate** task. The Deactivate Task Confirmation window is displayed.

Note: If one or more of the selected CPCs have associated secondary objects (for example, an image or coupling facility image), a Secondary Object Notification for Disruptive Task message window is displayed with a list of the active secondary objects. Review the list before proceeding. If you click **Yes** to proceed, the Deactivate Task Confirmation window is displayed. If you click **Yes** to proceed the Disruptive Task Confirmation window is displayed. Review the confirmation text to decide whether or not to proceed with the task.

3. Review the information on the window to verify that the object(s) you will deactivate is the correct one. If you want to continue this task, click **Yes**. If you want to end the task, click **No**. If you click **Yes**, the Deactivate Progress window is displayed.
4. The Deactivate Progress window is displayed indicating the progress of the deactivation and the outcome. 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.

Grouping



Notes:

- If Customizable Data Replication is *Enabled* on this Hardware Management Console (using the **Configure Data Replication** task), the data 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” on page 86.
- See “Grouping” on page 196 when you are managing z/VM virtual machines from the Hardware Management Console.

This task enables you to create, delete, add to, or delete from user-defined groups of objects. When you select one or more CPCs, CPC images, or groups and open the **Grouping** task, the Manage Groups window is displayed, allowing you to specify what type of action you want to take on the group. You can create a group when you want to perform the same task on several CPCs or CPC images simultaneously instead of repeating the task on each individual CPC or CPC image. You can also create groups when managing multiple sysplexes by creating a group for each sysplex controlled by the Hardware Management Console.

You can also create a *Pattern Match* group. A *Pattern Match* group is a group that contains all managed objects of a given type (custom groups, defined CPCs, images, director/timer consoles, IBM fiber savers, or z/VM virtual machines) whose names match a certain pattern (for example, all CPCs starting with P0).

To create a group with all CPCs starting with P0:

1. Select the object or objects you want to work with, then open the **Grouping** task. The Manage Groups window is displayed. Select **Create a new pattern match group** on the Manage Groups window, then click **OK**. The Create Pattern Match Group window is displayed.
Or, you can open the **Grouping** task without selecting an object or objects. The Create Pattern Match Group window is displayed.
2. As shown in Figure 50 on page 141, select the **Group type** you are creating.
3. Specify *P0group* in the **New group name** field and add a description of the group in the **New group description** field.
4. Specify *P0.** in the **Managed Resource Pattern** field on the **Create Pattern Match Group** window, then click **OK**.
5. You receive a message that the group (*P0group*) is created and the selected objects are added to it.

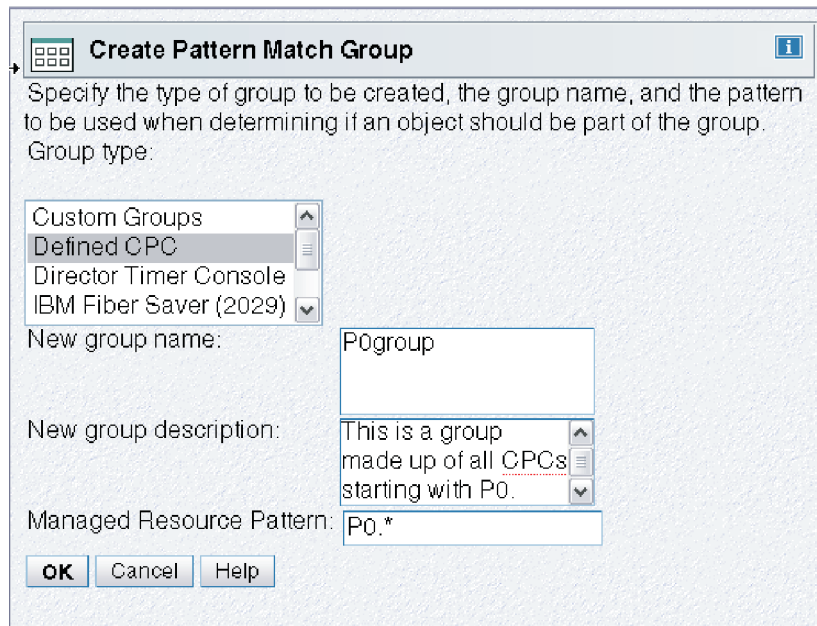


Figure 50. Create pattern match group window

Any new groups that you create are displayed in the **Groups Work Area** for the classic interface and in **Custom Groups** under the **Systems Management** node for the tree interface. Also, an entry is displayed in the **Customize User Controls** task in the Manage Resource Roles table that indicates a group has been added. The entry is **Groups created by userid**, where *userid* is the name of the user that created the group.

To group CPCs or CPC images:

1. Open the group that contains the CPCs or images that you want to group.
2. Select one or more objects.
3. Open the **Grouping** task under **Daily**.
4. The Manage Groups window is displayed allowing you to add the selected object or objects to an existing group, remove the selected object or objects from a group, create a group, create a pattern match group, remove the group, create another pattern match group, or edit an existing pattern match group.

This task also allows you to group one or more user-defined groups into other groups. You might want to do this 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 CPCs and/or CPC images:

1. Select one of the groups you want to group together.
2. Open the **Grouping** tasks under **Daily**. The **Manage Groups** window is displayed.
3. Select **Create a new group**.
4. Enter a *group name* in the **New group name** input field and a description in the **New group description** input field. The description is used when hover help is set in the classic style user interface.
5. Click **OK**. The Create a New Group window is displayed stating that you have successfully created a group.
6. Click **OK**. The new group is now displayed in the **Groups Work Area** in the classic interface or under **Custom Groups** in the tree interface.

7. Select another group that you want to add to the group you just created.
8. Open the **Grouping** task under **Daily**. The Manage Groups window is displayed.
9. Select **Add to an existing group**.
10. Select the *group name* you created in **step 4** from the **Group Name** field.
11. Click **OK**. The Add to an Existing Group window is displayed stating that you have successfully added a group to another group.
12. Click **OK**. The group is no longer displayed in the **Groups Work Area** in the classic interface or **Custom Groups** in the tree interface because it is now part of the group you created in **step 4**.
13. Repeat **steps 7 through 12** for as many groups that you want to add to the new group.

As previously stated, you cannot perform tasks on grouped groups. They can only be performed on the group that contains the individual CPCs or CPC images. You can get access to this group or the individual CPCs or CPC images in the group using one of the following classic interface methods:

- Double-click the grouped icon in the **Groups Work Area**. This opens up the groups that are nested in the preceding group. Continue double-clicking each nested group until the group that contains the individual CPCs or CPC images is displayed, or
- Open the workplace pop-up menu
 1. Right-click on any empty area in the workplace. This opens the workplace pop-up menu.
 2. Point to **Groups** to open its cascaded menu. Continue selecting each cascaded menu until the individual group that contains the CPCs or CPC images that you want to perform an action on is displayed and click that item.

Or by using one of the following tree interface methods:

- Click the group under the **Custom Groups** node in the navigation pane that you want to work with. This expands to show the groups that are nested within that group. Continue to click each nested group until the group that contains the individual servers is displayed in the work pane.
- Continue to click the group name from the work pane until the individual servers are displayed.

Use the online Help if you need additional information for working with groups.

Reset Normal



Notes:

- This task is supported only for CPC image objects or groups of CPC images.
- Reset Normal is considered a disruptive task. If the object is locked, you must unlock it before continuing. For more information about disruptive tasks, see “Disruptive tasks” on page 6.

This task terminates any current operations and clears any interruption conditions in a CPC image (except for a coupling facility image). A reset normal does not clear main storage during initialization.

To perform a Reset Normal:

1. Select one or more CPC images.
2. Open the **Reset Normal** task. The Reset Normal Task Confirmation window is displayed.
3. Review the information on the window to verify that the object(s) you will reset is the correct one. If the information is correct, click **Yes**. The Reset Normal Progress window displays indicating the progress of the reset and the outcome.
4. Click **OK** to close the window when the reset completes successfully.

Level 01a

Otherwise, if the reset does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

Recovery



Recovery tasks are used to recover from a suspected CPC hardware or software error.

The following are represented in the *Recovery* tasks:

- Access Removable Media
- Integrated 3270 Console
- Integrated ASCII Console
- Load
- Load from Removable Media or Server
- PSW Restart
- Reset Clear
- Reset Normal
- Single Object Operations
- Start All
- Stop All

Access Removable Media



Use this task for installing Linux, or other software as specified in its information from removable media (DVD-RAM, USB flash memory drive, or diskette (if one is available)) as a guest of z/VM, if the z/VM support running in the logical partition supports this capability. This task is available only on System z10 or later.

To install Linux or other software from removable media as a guest of z/VM:

1. Properly insert a DVD-RAM, USB flash memory drive (see “USB flash memory drive” on page 10 for more information) or a diskette (if one is available).
2. Select a partition.
3. Open the **Access Removable Media** task. The Access to Removable Media window is displayed.
4. Select the removable media that you want the specified partition to access, then insert the media into the Hardware Management Console.
5. Click **OK** to proceed with assigning the selected removable media for use by the partition. The confirmation window is displayed.

Use the online Help if you need additional information for installing Linux or other software.

Integrated 3270 Console



Notes:

- This task is supported by z/VM 4.4 or later.
- One 3270 console is available for each CPC image.

This task provides a 3270 console that can be used with a host operating system without the need for any special connectivity or additional hardware, such as control units or network connections. The Integrated 3270 Console uses the already existing network connection between the Hardware Management Console and the Support Element, and the connection between the Support Element and the CPC to connect with the host operating system.

To start the console:

1. Select a CPC image.
2. Open the **Integrated 3270 Console** task. The Integrated 3270 Console window is displayed.

An X SYSTEM indicator will also display in the Status area. If the host operating system is already started, the Integrated 3270 Console task will try to establish communications with it. After the host system responds, the Integrated 3270 Console window will be updated with data provided by the host operating system. If the host system is not running or does not support the Integrated 3270 Console, then the Integrated 3270 Console window will remain blank.

If the host system is not running, close the blank window, then you can start the system by performing the **Load** task (see "Load" on page 146).

- a. With the object still selected, open the **Load** task (under the Recovery task group).
- b. The Load window is displayed.
- c. Enter the *load address* of your operating system in the **Load address** input field.
- d. Enter the *load parameter* (for example, **SYSG** for zVM4.4) in the **Load parameter** input field.
- e. Click **OK**. The Load Task Confirmation window is displayed.
- f. Click **Yes**. The Load Progress window is displayed indicating the progress of the load and the outcome.
- g. Click **OK** to close the window when the load completes successfully.
- h. After the load completes, select the object again, open the **Integrated 3270 Console** task. The Integrated 3270 Console window is displayed and updated with data provided by the host operating system.
3. Click the X in the upper right corner of the window when you are done working with the console.

Use the online Help if you need additional information for using the Integrated 3270 Console.

Integrated ASCII Console



Notes:

- This task is supported by the Linux operating system running in an LPAR partition or as a guest of z/VM (Version V5.3 or later).
- One ASCII console is available for each CPC image.

This task provides an ASCII console that can be used with a host operating system without the need for any special connectivity or additional hardware, such as control units or network connections. The Integrated ASCII Console uses the already existing network connection between the Hardware Management Console and the Support Element, and the connection between the Support Element and the CPC to connect with the host operating system.

To start the console:

1. Select a CPC image.
2. Open the **Integrated ASCII Console** task. The Integrated ASCII Console window is displayed.

If the Linux operating system is already started, the Integrated ASCII Console task will try to establish communications with it. After the operating system responds, press Enter, the Integrated ASCII Console window will be updated with the Linux Welcome screen.

If the Linux operating system is not running, you can start the system by performing the **Load** task (see “Load”).

- a. With the CPC still selected, open the **Load** task (under the Recovery task group).
 - b. The Load window is displayed.
 - c. Enter the *load address* of your operating system in the **Load address** input field.
 - d. Click **OK**. The Load Task Confirmation window is displayed.
 - e. Click **Yes**. The Load Progress window is displayed indicating the progress of the load and the outcome.
 - f. Click **OK** to close the window when the load completes successfully.
 - g. After the load completes, select the CPC again, open the **Integrated ASCII Console** task. The Integrated ASCII Console window is displayed and updated with the Linux Welcome screen.
3. Click the **X** in the upper right corner of the window when you are done working with the console.

Use the online Help to get additional information on starting an ASCII console session.

Load



Notes:

- Depending on your machine type, model, and features installed, you can have up to four Load types:
 - Normal
 - Clear
 - SCSI
 - SCSI dump.

If you have a z800 or z900 with the SCSI IPL feature installed, you must first select **Enable SCSI IPL** on the Options window of the Reset Profile from the **Customize/Delete Activation Profiles** task and then IML the system. Otherwise, the SCSI load or SCSI dump will not work properly. (See “Customize/Delete Activation Profiles” on page 174 for more information.)

- 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.
- Other products and documentation may refer to this operation as an *initial program load (IPL)*.
- Load is considered a disruptive task. If the object is locked, you must unlock it before continuing. For more information about disruptive tasks, see “Disruptive tasks” on page 6.

Load (except for a coupling facility image) causes a program to be read from a designated device and initiates running that program. If the CPC is operating in logically partitioned (LPAR) mode, the logical partition is the target of the load. Otherwise, if the CPC is operating in basic mode, the CPC is the target of the load.

To perform a load:

1. Select one or more CPC images.
2. Open the **Load** task. The Load window is displayed with the information that was last used when the CPC image was loaded.
3. 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 the Disruptive Task Confirmation window is displayed. Review the confirmation text to decide whether or not to proceed with the task.

4. To continue with the load, click **Yes**. The Load Progress window is displayed indicating the progress of the load and the outcome.
5. 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.

Use the online Help to get additional information for loading a CPC image.

Load from Removable Media or Server



Note: Load from Removable Media or Server is considered a disruptive task. If the object is locked, you must unlock it before continuing. For more information about disruptive tasks, see “Disruptive tasks” on page 6.

This task loads system software or utility programs from a CD-ROM, DVD, USB flash memory drive, a local removable media device, or from an FTP server.

To load the software:

1. Select a CPC image.
2. Open the **Load from Removable Media or Server** task. The Load from Removable Media or Server window is displayed.
3. Select one of the software options:
 - Hardware Management Console CD-ROM/DVD
 - Hardware Management Console CD/DVD and assign for operating system use
 - Hardware Management Console USB flash memory drive (see “USB flash memory drive” on page 10 for more information)
 - Hardware Management Console USB flash memory drive and assign for operating system use
 - Local removable media device
 - FTP Source (If you choose this option specify the FTP host computer, user ID, password, and account.)

Then, click **OK** to continue.

4. The Load from Removable Media or Server window is displayed. Select the software or utility program you want to load, click **OK** to continue. A progress window displays the duration and elapsed time of the program loaded.
5. Click **OK** to close the window when the task completes successfully.

Use the online Help to get additional information for loading from a removable media or server.

PSW Restart



Note: PSW Restart is considered a disruptive task. If the object is locked, you must unlock it before continuing. For more information about disruptive tasks, see “Disruptive tasks” on page 6.

This task performs a restart operation on the first available central processor(s) of the selected CPC images (except for a coupling facility image).

A restart interruption will store the current program status word (PSW) at real address 8 and fetch a new PSW from real address 0 in central storage.

PSW Restart can be used when the status of the selected object is:

- Operating
- Stopped

To restart a processor:

1. Select a CPC image.
 2. Open the **PSW Restart** task. The PSW Restart Task Confirmation window is displayed.
 3. If you click **Yes** to proceed with the task, the Disruptive Task Confirmation window is displayed. Review the confirmation text to decide whether or not to proceed with the task.
 4. To continue with the restart, click **Yes**. The PSW Restart Progress window is displayed indicating the progress of the restart and the outcome.
 5. 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.

Reset Clear



Notes:

- This task is supported only for CPC image objects or groups of CPC images.
- Reset Clear is considered a disruptive task. If the object is locked, you must unlock it before continuing. For more information about disruptive tasks, see “Disruptive tasks” on page 6.

This task terminates any current operations and clears any interruption conditions in a CPC image (except for a coupling facility image). A reset clear clears main storage and all registers during initialization.

To perform a reset:

1. Select a CPC image.
 2. Open the **Reset Clear** task. The Reset Clear Task Confirmation window is displayed.
 3. If you click **Yes** to proceed with the task, the Disruptive Task Confirmation window is displayed. Review the confirmation text to decide whether or not to proceed with the task.
 4. To continue with the reset, click **Yes**. The Reset Clear Progress window is displayed indicating the progress of the reset and the outcome.
 5. Click **OK** to close the window when the reset completes successfully.
- Otherwise, if the reset does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

Reset Normal



Notes:

- The Reset Normal task is supported only for CPC image objects or groups of CPC images.
- Reset Normal is considered a disruptive task. If the object is locked, you must unlock it before continuing. For more information about disruptive tasks, see “Disruptive tasks” on page 6.

This task terminates any current operations and clears any interruption conditions in a CPC image (except for a coupling facility image). A reset normal does not clear main storage during initialization.

To perform a reset normal:

1. Select a CPC image.
2. Open the **Reset Normal** task. The Reset Normal Task Confirmation window is displayed.
3. If you click **Yes** to proceed with the task, the Disruptive Task Confirmation window is displayed. Review the confirmation text to decide whether or not to proceed with the task.
4. To continue with the reset, click **Yes**. The Reset Normal Progress window is displayed indicating the progress of the reset and the outcome.
5. Click **OK** to close the window when the reset completes successfully.
Otherwise, if the reset does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

Single Object Operations



Notes:

- The following steps are used when trying to determine the correct authorization level used for the Single Object Operations session:
 - If the same user ID is defined on the target object, then the authorization level for that user will be used.
 - Otherwise, the authority of the *user mode* that corresponds to the "most powerful" task role associated with the user is used. The *user mode* is determined by working back to the predefined task roles associated with the user.
- Only one direct connection, through this task, can be initiated at a time, and a maximum of four can be active at any one time. Only one Single Object Operations session can be active for any Support Element.
- If your Hardware Management Console (Version 2.10.0 or later) does not have a diskette drive then any Support Element (Version 2.9.2 or earlier) task that tries to access the Hardware Management Console diskette drive will be redirected to access a USB flash memory drive (see “USB flash memory drive” on page 10 for more information).
- This task can also be performed on a defined director/timer.

This task creates a direct connection to a single object Support Element. You may need to connect to an individual Support Element to investigate and resolve exception situations. After a Single Object Operations session has been established, you can control the input to the Support Element or just monitor the output of the Support Element by using the **Session** pull down on the window.

See the *Support Element Operations Guide* for a description of the functions that can be performed using this task.

Note: For all Support Elements at Version 2.10.0 or later all change internal code function must be performed from the Hardware Management Console using the **Change Internal Code** task.

To establish a Support Element session from the Hardware Management Console:

1. Select a CPC (server) or director/timer.
2. Open the **Single Object Operations** task. The Single Object Operations Task Confirmation window is displayed.
3. Click **Yes** to proceed or **No** to go back to the Hardware Management Console workplace.
4. If you click **Yes**, the Support Element workplace is displayed and you can proceed with the appropriate tasks.

Note: If the Support Element you attempt to connect to is already established, a message is displayed. You have the option to click **Close** and return to the Hardware Management Console workplace or you can click **Chat** to open the **Console Messenger** task and initiate a chat session with the user session on the Support Element.

5. Click the red X in the upper right corner of the workplace to end the session and go back to the Hardware Management Console workplace.

Start All



Note: Start is considered a disruptive task. If the object is locked, you must unlock it before continuing. For more information about disruptive tasks, see “Disruptive tasks” on page 6.

This task ends instruction stop state for selected CPC images (except for a coupling facility image) that were previously stopped. This causes instruction processing to begin.

To start CPC images:

1. Select a CPC image.
2. Open the **Start All** task. The Start All Task Confirmation window is displayed.
3. If you click **Yes** to proceed with the task, the Disruptive Task Confirmation window is displayed. Review the confirmation text to decide whether or not to proceed with the task.
4. To continue with the start, click **Yes**. The Start All Task Progress window is displayed indicating the progress of the start and the outcome.
5. Click **OK** to close the window when the start completes successfully.

Otherwise, if the stop does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

Stop All



Note: Stop is considered a disruptive task. If the object is locked, you must unlock it before continuing. For more information about disruptive tasks, see “Disruptive tasks” on page 6.

This task places all selected CPC images (except for a coupling facility image) in an instruction stop state. This changes the operational status to **Stopped**.

To stop CPC images:

1. Select a CPC image.
2. Open the **Stop All** task. The Stop All Task Confirmation window is displayed.
3. If you click **Yes** to proceed with the task, the Disruptive Task Confirmation window is displayed. Review the confirmation text to decide whether or not to proceed with the task.
4. To continue with the stop, click **Yes**. The Stop All Task Progress window is displayed indicating the progress of the stop and the outcome.
5. Click **OK** to close the window when the stop completes successfully.
Otherwise, if the stop does not complete successfully, follow the directions on the window to determine the problem and how to correct it.

Service



Service tasks are used to analyze suspected hardware errors and report problem data to IBM, backup critical CPC data, and archive security log files. Additional *Service Representative* tasks are available to test the processor cluster hardware and to restore Support Element licensed internal code.

The following are represented in the *Service* tasks:

- Archive Security Logs
- Backup Critical Data
- Perform Problem Analysis
- Perform Transfer Rate Test
- Report a Problem
- Restore Critical Data
- Service Status
- Transmit Service Data
- View PMV Records
- View Service History

Archive Security Logs



Notes:

- The DVD-RAM or USB flash memory drive used for archiving security logs must be formatted with a volume label of **ACTSECLG**.
- If you are using a USB flash memory drive it must have a capacity of 1 GB or greater.
- You cannot perform this task remotely.

This task archives a security log for a CPC. Up to ten CPC security logs can be archived at one time. When the Archive Security Logs window is displayed, verify that the CPC shown in the window list is the one whose security log you want to archive.

To archive a security log:

1. Select one or more CPCs.
2. Open the **Archive Security Logs** window. The Archive Security Logs window is displayed.
3. Verify the CPC(s) shown in the Archive Security Logs window list is the one whose security log you want to archive.

Note: Ensure that the DVD-RAM or USB flash memory drive that you are using for archiving is inserted properly. (See “USB flash memory drive” on page 10 for more information.)

4. Click **Archive**, choose the mass rewritable media (DVD-RAM or USB flash memory drive) to archive to from the Select Media Device window, then click **OK** to start the procedure.

Use the online Help if you need additional information for archiving a CPC security log.

Backup Critical Data



Note: The USB flash memory drive used for the **Backup Critical Data** task must be formatted with a volume label of **ACTBKP**.

This task transfers critical CPC data that is stored on its Support Element to the Hardware Management Console and copies it to removable media. CPC data should be backed up when configuration or CPC licensed internal code changes have been made or as a routine preventive maintenance procedure.

To back up critical CPC data stored on its Support Element:

1. Select one or more CPCs.
2. Open the **Backup Critical Data** task. The Backup Critical Data Confirmation window is displayed.
3. Insert the backup USB flash memory drive in the Hardware Management Console if it is not already in place. (See “USB flash memory drive” on page 10 for more information.)
4. Click **Backup** to begin.
5. The Backup SE Critical Data Progress window is displayed.
6. When back up is complete, click **OK**.

Use the online Help if additional information is needed in backing up the Support Element's critical data.

Perform Problem Analysis



This task manually calls Problem Analysis, which analyzes stored data that is collected from various parts of a processor at the time of an error and determines the type of problem. Problem Analysis then informs the user of the steps that are necessary to resolve the problem.

Problems that are considered to be *hard* errors start Problem Analysis automatically. An example of a hard error is a processor card failure. Results from automatic Problem Analysis are stored under **Hardware Messages**.

The icon of the CPC that had the hard error and the icon of any group that contains the CPC icon will have a blue background indicating that Problem Analysis results were reported for that CPC.

Problems that can be considered to be *soft* errors require the operator to start Problem Analysis manually, usually after the operating system reports a problem. An example of a soft error is an interface control check (IFCC).

To perform a manual problem analysis:

1. Select one or more CPCs (servers).
2. Open the **Perform Problem Analysis** task. The Problem Analysis window is displayed. This window displays the last 50 IFCCs that occurred.
3. You can select a specific problem, then click **View Selected Errors....** The Problem Analysis window is displayed listing a description of the errors for the problem you previously selected.
4. You can continue to analyze the problems or click **Cancel** to return to the previous window.

Use the online Help for additional information to manually start problem analysis.

Perform Transfer Rate Test



This task decides whether you want to perform the transfer rate test for a selected object to the primary Support Element or to the alternate Support Element.

To perform the transfer rate test:

1. Select a CPC (server).
2. Open the **Perform Transfer Rate Test** task. The Perform Transfer Rate Test message window is displayed.
3. Click **Primary** to test against the primary Support Element or click **Alternate** to test against the alternate Support Element.
4. Click **Cancel** to exit the task without performing the transfer rate test.

Report a Problem



This task allows you to report a problem on the CPC. You should use this task only when there are no Problem Analysis results for the problem.

If Problem Analysis results do exist, report the problem by clicking the **Service** on the Hardware Messages window associated with the problem. If Problem Analysis was not invoked automatically, use the **Perform Problem Analysis** task to attempt to resolve the problem without a request for service.

You can also use this task to test problem reporting.

To report a problem on a CPC:

1. Select a CPC (server).
2. Open the **Report a Problem** task. The Report a Problem window is displayed.
3. Select the type of problem from the list provided and enter a brief description of your problem in the **Problem Description** input field, then click **Request Service**.
4. Click **Request Service**.

To test whether problems can be reported you can perform the following:

1. Select **Test automatic problem reporting** from the Report a Problem window and enter **This is just a test** in the **Problem Description** input field.
2. Click **Request Service**. The Report Problem message window is displayed.
3. Click **OK** to complete the task.

Use the online Help if additional information is needed to report the problem and request service.

Restore Critical Data



Notes:

- This task is not available for CPCs that were defined using the CPC Manual Definition Template.
- You cannot perform this task remotely.

This task initializes the hard disk, installs the internal code, and restores critical CPC data from removable media to the Support Element of the selected CPC. The critical CPC data that is restored to the Support Element is the data that was copied to the removable media by using the **Backup Critical Data** task.

In order to perform this task you need the following pieces of media:

- Backup DVD-RAM or USB flash memory drive (see “USB flash memory drive” on page 10 for more information) that contains the backup critical data for this particular CPC object
- Support Element restore diskette
- Support Element DVD AROM.

To restore critical data to a Support Element:

1. Select one or more CPCs (servers).
2. Open the **Restore Critical Data** task. The Confirm the Action window is displayed.
3. Insert the backup media, then click **Restore**.

Use the online Help to get additional information for restoring critical data to a Support Element.

Service Status



This task sets a CPC to Service Status allowing a service representative to perform service tasks on the CPC or Support Element. Many of the CPC service tasks require that the CPC is first placed in Service Status. Repair and Verify, for example, cannot be run on a CPC until that CPC is placed in Service Status.

Service Status should be enabled for CPCs that are to be serviced. When in Service Status, the CPC status displayed on its Details window will be Service and no other status will be reported by the CPC 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. CPC images will not be displayed on the Hardware Management Console when Service Status is enabled for the CPC.

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 CPCs (servers).
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**.

Use the online Help if you need additional information for placing the CPC in service status.

Transmit Service Data



Note: If you want to access this task remotely you must enable access to the IBM remote support system.

This task allows you to send service data to IBM either by copying it to a DVD-RAM, diskette (if one is available), or USB flash memory drive for delivery to IBM, or by transmitting it to IBM through a remote connection to the IBM Service Support System. (See “USB flash memory drive” on page 10 for more information.)

Sending service data to IBM is necessary only when service data is requested by IBM, usually through either your service representative or the IBM Service Support System. Typically, IBM will request service data after a problem is reported if analyzing the service data is necessary to determine the cause of the problem.

Service data is a set of system information, such as program and event traces, collected by the CPC's Support Element. When IBM is your service provider for the CPC, service data assists IBM in servicing it.

To send the Support Element's service data to IBM:

1. Select a CPC (server).
2. Open the **Transmit Service Data** task. The Transmit Service Data to IBM window is displayed.
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. Select the data you want to send and the destination for the data, enter the related problem management number if it is known, and you can select **zBX Resources** to send if the IBM zEnterprise BladeCenter Extension (zBX) feature is installed.
5. Click **Send** to transmit the selected data or **Cancel** to end the task without sending any data.

Use the online Help if additional information is needed to send service data.

View PMV Records



This task allows you to obtain the Problem Management Viewable (PMV) records issued to the IBM Service Support System for one or more CPC Support Elements. These problems are typically sent to the IBM Service Support System where errors are not recorded by the console. You are able to view and edit the PMV records on the console and you have the ability for an interactive dialog with an IBM service representative. A PMV record is initially created from the **Report a Problem** task specifying a problem type of **Type V Viewable PMH(PMV)**.

To view a PMV record:

1. Select one or more CPCs (servers).
2. Open the **View PMV Records** task. The View PMV Records window is displayed.
3. Click **Yes** to retrieve a list of the most recent records, otherwise click **No** to get a list of records without the latest updates. The View PMV Records message window is displayed. It indicates the PMV records that are being retrieved from the IBM Service Support System. This process can take a long time. You can click **Cancel** to stop the process and exit the task at any time.
4. When the records have been retrieved, the View PMV Records window displays a listing of the PMV records and corresponding machine.
5. Select a PMV record to view, click **View PMV**. A message is displayed indicating the retrieval of the PMV record. The View PMV Records window is displayed. From this window the following options are available:
 - To add a comment to the PMV record, click **Add Comment**. The View PMV Records window is displayed with a text input area. Provide a comment in the text input area and click **Add Comment**.
 - To refresh the details of the PMV record, click **Refresh PMV**. The PMV record displays the most current information.
 - To supply a screen capture of the problem in the PMV record, click **Add Attachment**. The View PMV Records window is displayed with the available screen captures you created using the **Manage Print Screen** task. Select one or more files and click **Upload Image**.
 - To view existing screen captures (files) available for download, click **View Available Attachments**. The View PMV window displays a list of attachments that can be downloaded for the PVM record. Select one or more attachments you want to download then click **Download Attachment**.
 - To view attachments on the PVM record, click **View Downloaded Attachments**. The View PMV Records window displays the screen captures you uploaded to the PVM record. To view an image, select one then click **View Image**.
6. To stop processing an action on a PVM record or to exit the task, click **Cancel** at any time.

Use the online Help if you need additional information for viewing PMV records.

View Service History



This task displays a list of current problems for selected CPCs or a selected group of CPCs. The problems may be opened or closed and will be displayed with the most recent entry at the top of the list.

To display the service history:

1. Select one or more CPCs (servers).
2. Open the **View Service History** task. The Service History window is displayed.
3. 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.
 - 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.

4. When you have completed this task, select **View, Exit** to return to the Hardware Management Console workplace.

Use the online Help for additional information about the problem and the service information on it.

Change Management



Change Management tasks are used to work with the licensed internal code of Support Elements in the processor cluster.

Note: Only CPCs that are defined will receive licensed internal code updates. If you intend to update the Support Element licensed internal code of all of the CPCs in a processor cluster, verify that all of the CPCs are defined to the Hardware Management Console.

The following are represented in the *Change Management* tasks:

- Alternate Support Element
- Alternate Support Element Engineering Changes (ECs)
- Change Internal Code
- Concurrent Upgrade Engineering Changes (ECs)
- Engineering Changes (ECs)
- Product Engineering Directed Changes
- Retrieve Internal Code
- Save Legacy Upgrade Data
- Single Step Internal Code Changes
- Special Code Load
- System Information

Alternate Support Element



Notes:

- Each CPC must be a model that has both a primary and alternate Support Element installed.
- The primary Support Element 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.

This task performs 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.

Mirroring the primary Support Element data to the alternate Support Element

Mirroring Support Element data copies the data from a CPC's primary Support Element to its alternate Support Element. By regularly mirroring primary Support Element data, you help ensure the alternate Support Element will function the same as the primary Support Element in case you need to switch the alternate Support Element to become the primary Support Element (for example, because of a hardware failure on the existing primary Support Element).

Ordinarily, Support Element data is mirrored automatically each day at 10:00 a.m., but you can use this task 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
- Creating, changing, or deleting groups
- Automatic activation.

To mirror the primary Support Element data:

1. Select one or more CPCs (servers).
2. Open the **Alternate Support Element** task. The Alternate Support Element window is displayed.
3. Select **Mirror the Primary Support Element data to the Alternate Support Element**.
4. Click **OK** to begin mirroring.

Use the online Help if you need additional information for mirroring the Support Element.

Switching to the alternate Support Element

Do this when you need to switch the alternate Support Element to become the primary Support Element. When a manual switchover is started, the system checks that all internal code level information is the same on both Support Elements 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 powered off before completing the switch. The following are several conditions that will prevent a switchover:

- Mirroring task in progress
- Internal code update
- Hard disk restore
- Engineering change
- Concurrent upgrade engineering changes preload condition.

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.

To switch to the alternate Support Element from the Alternate Support Element window:

1. Select one or more CPCs (servers).
2. Open the **Alternate Support Element** task. The Alternate Support Element window is displayed.
3. Select **Switch the Primary Support Element and the Alternate Support Element**.
4. Click **OK** to switch to the alternate Support Element.
5. A confirmation window is displayed.

Use the online Help if you need additional information for switching to the alternate Support Element.

Querying switch capabilities between Support Elements

The querying switch capability provides a quick check of the communication path between the Support Elements, the status of the Support Elements, and the status of the automatic switch action. You may want to perform this action before attempting to switch to the alternate Support Element.

To query switch capabilities from the Alternate Support Element window:

1. Select one or more CPCs (servers).
2. Open the **Alternate Support Element** task. The Alternate Support Element window is displayed.
3. Select **Query Switch capabilities**.
4. Click **OK** to start the query.
5. A confirmation window is displayed.

Use the online Help if you need additional information for querying switching capabilities.

Alternate Support Element Engineering Changes (ECs)



Notes:

- This task is available only on a CPC that has both a primary and an alternate Support Element.
- You cannot perform this task remotely.

This task upgrades the alternate Support Element of the selected CPC. You can perform any of the following options:

Upgrade Alternate SE (Preload)

Upgrade both the operating system and the Support Element function code to the alternate Support Element.

Alternate SE - Retrieve and Activate MCLs from Retain

Retrieve and activate microcode level (internal code change) updates obtained from the IBM Service Support System to the alternate Support Element.

Upgrade Alternate SE (Preload) and then Retrieve and Activate MCLs from Retain

Upgrade both the operating system and the Support Element function code. Then, retrieve and activate internal code change updates to the alternate Support Element.

Alternate SE - Retrieve and Activate MCLs from removable media

Retrieve and activate microcode level (internal code change) updates obtained from removable media (USB flash memory drive) to the alternate Support Element. (See “USB flash memory drive” on page 10 for more information.)

To upgrade the alternate Support Element:

1. Select a CPC (server).
2. Open the **Alternate Support Element Engineering Changes (EC)** task. The Upgrade Engineering Change (EC) - Alternate SE window is displayed.
3. Select the engineering change option you want to perform, then click **OK**. The Apply Changes Confirmation window is displayed.
4. The processor or processors to change are listed. Click **OK** to confirm performing the update.

Use the online Help for additional information on upgrading the alternate Support Element.

Change Internal Code



Note: Change Internal Code is considered a disruptive task. If the object is locked, you must unlock it before continuing. For more information about disruptive tasks, see “Disruptive tasks” on page 6.

This task enables you to modify CPC internal code which may provide new operations, or correct or improve existing operations. Also, any Support Element at Version 2.10.0 or later must use this task for all change internal code functions.

You can modify the internal code of:

- All defined CPCs
- All CPCs in a user-defined group
- Selected individual CPC or CPCs.

You can:

- Accept installed changes that were activated
- Install and activate changes that were retrieved
- Browse system and internal code information
- Remove and activate changes
- Delete all retrieved changes that were not installed.

An IBM service representative will provide new internal code changes and manage their initial use. For internal code changes already stored on your hard disk, IBM recommends that you manage these changes only under the supervision of an IBM service representative or with the assistance of your IBM Service Support System.

Certain licensed internal code changes may require the MRU to shut down during the activation of the change. This is normal for these changes. This could cause a slight degradation in system performance during the time the MRU is shut down. After activation is complete, the MRU will be turned on again, and normal performance will be resumed.

To change the CPC internal code:

1. Select one or more CPCs (servers).
2. Open the **Change Internal Code** task. The Change Internal Code window is displayed.
3. Click the option you want to perform and then click **OK**.
4. Follow the instructions on the subsequent windows to complete the task.

Use the online Help if you need additional information in changing the internal code.

Concurrent Upgrade Engineering Changes (ECs)



Notes:

- The CPC(s) must be placed in Service Status before starting this task.
- You cannot perform this task remotely.

This task upgrades Engineering Changes (ECs) concurrently for a specified Central Processing Complex (CPC) eliminating the need for down time when you are adding the new functions.

To concurrently upgrade engineering changes:

1. Select a CPC (server).
2. Open the **Concurrent Upgrade Engineering Changes (EC)** task. The Concurrent Upgrade Engineering Changes window is displayed.

3. Choose the action to perform in the order as it is displayed.

Preload

Options for loading the engineering changes in order to upgrade the CPC to a new level.

Activate

After selecting a Preload option this action switches the CPC to a new level.

Query function availability from last activate

After activating the upgrade a table is displayed indicating new functions that were disabled or unavailable.

Query concurrent upgrade requirements

This option is available only for a System z10 or later CPC. It determines if the concurrent upgrade requirements have been met.

View summary of all minimum and maximum level requirements

Displays the minimum and maximum levels of internal code changes required for performing an upgrade with this task.

4. Click **OK** to proceed with the upgrade.

For more detailed information on the Concurrent Upgrade Engineering Changes (CUEC) and how to use this task, see Appendix B, “Enhanced driver maintenance,” on page 209. You can also use the online Help for additional information on concurrent upgrading for engineering changes.

Engineering Changes (ECs)



Notes:

- The CPC(s) must be placed in Service Status before starting this task.
- You cannot perform this task remotely.
- Engineering Changes (ECs) is considered a disruptive task. If the object is locked, you must unlock it before continuing. For more information about disruptive tasks, see “Disruptive tasks” on page 6.

This task copies base code ECs from a CDROM or DVD-RAM to the Hardware Management Console to install on the primary Support Element of a CPC. You can upgrade the primary Support Element in either of the following ways:

Upgrade primary SE

Upgrade both the operating system code and the Support Element function code. This option deactivates the CPC and stops all operating systems running on the CPC.

Upgrade primary SE operating system

Upgrade only the operating system code. This option can be run concurrent to the operating systems running on the CPC.

To upgrade the primary Support Element:

1. Select a CPC (server).
2. Open the **Engineering Changes (EC)** task. The Upgrade Engineering Change (EC) window is displayed.
3. Click the engineering change option you want to perform, then click **OK**. The Insert the SE-CD window is displayed.
4. Ensure that the CDROM or DVD-RAM is in the drive, and click **OK**.

Use the online Help for additional information for working with engineering changes.

Product Engineering Directed Changes



Notes:

- You cannot perform this task remotely.
- Product Engineering Directed Changes is considered a disruptive task. If the object is locked, you must unlock it before continuing. For more information about disruptive tasks, see “Disruptive tasks” on page 6.

This task enables the service representative to receive temporary licensed internal code fixes when no formal changes are available. This task should be used only when IBM Product Engineering directs you to do so. The following selections are available from the menu:

To receive temporary licensed internal code fixes:

1. Select one or more CPCs (servers).
2. Open the **Product Engineering Directed Changes** task. The Product Engineering Directed Changes window is displayed.
3. Select one of the following options:

Retrieve all temporary internal code fixes

Use this selection to retrieve an internal code fix from removable media (DVD-RAM, USB flash memory drive, or diskette (if one is available)) See “USB flash memory drive” on page 10 for more information. The fix is then stored on the Support Elements for the selected CPCs. The fix is also stored in a staging area on the Hardware Management Console hard drive.

Note: A set of fixes is stored in the Hardware Management Console fixed drive staging area during a retrieve. This set of fixes is available there for other CPCs until a different set of fixes is retrieved. The fixes may also be placed in the staging area from a remote console.

Activate all temporary internal code fixes

Use this selection to replace the system's existing internal code with the retrieved internal code fixes when the system is activated. This changes the status on the Support Element Analyze Internal Code Changes window.

Deactivate and delete all temporary internal code fixes

Use this selection when a previously activated internal code fix is **not** to be used as a part of a CPC's internal code the next time the system is activated. This changes the status on the Support Element Analyze Internal Code Changes window.

4. Click **OK** to continue with the task or click **Cancel** to return to the Hardware Management Console workplace.

Use the online Help to get additional information for receiving engineering changes.

Retrieve Internal Code



Note: You can perform this task remotely **only** when you are retrieving data from the IBM Service Support System to a selected CPC.

This task copies internal code changes from the selected source to a Hardware Management Console work space and distributes updates to the Support Elements of CPCs defined to the Hardware Management Console. This task is to be used when you are working with internal code changes for the CPC Support Elements. Changes to the Hardware Management Console internal code are controlled using the **Change Console Internal Code** task.

To retrieve internal code changes:

1. Select one or more CPCs (servers).
2. Open the **Retrieve Internal Code** task. The Retrieve Internal Code Changes window is displayed.
3. Choose to work with all CPCs or selected CPCs:

Selected CPCs

Distributes code changes only to selected CPCs.

All CPCs

Distributes code changes to all defined CPCs.

The Retrieve Internal Code Changes window is displayed.

4. You can retrieve changes from the following sources and to the following targets.

Retrieve code changes from removable media to the selected objects

Select this when IBM has delivered the internal code changes to you on removable media (DVD-RAM, USB flash memory drive, or diskette (if one is available)) for a CPC Support Element. (See “USB flash memory drive” on page 10 for more information.)

Retrieve code changes from FTP site to the selected objects

Select this when IBM has internal code changes available to you from an FTP site for a CPC Support Element. You also have the option to enable a secure data transfer.

Retrieve code changes from IBM support system to the selected objects

Select this when IBM has notified you that new internal code changes are available through the IBM Service Support System and you want to retrieve the changes to the selected CPC Support Element.

Retrieve code changes to all Hardware Management Consoles also

Select this option to distribute code changes to the hard disk of all known Hardware Management Consoles, at Licensed Internal Code Version 2.9.2 or later, that are connected to the same LAN network as the selected CPCs.

Note: An IBM service representative will provide new internal code changes and manage their initial use. For internal code changes already stored on your hard disk, IBM recommends that you manage these changes only under the supervision of an IBM service representative or with the assistance of your IBM Service Support System.

Retrieving internal code changes only copies them from the source to the Support Element hard disk. Retrieved internal code changes do not affect the operation of your processor cluster until you install and activate them using the controls under the **Change Internal Code** task.

5. Click **OK** to proceed through the task windows.

Use the online Help to get additional information for retrieving internal code changes.

Save Legacy Upgrade Data



This task transfers 206X or 208X Support Element MES upgrade data from the Support Element to the Support Element's Upgrade Data DVD-RAM. It also transfers 209X Support Element MES upgrade data

from the Support Element to the Support Element's Upgrade Data USB flash memory drive. (See "USB flash memory drive" on page 10 for more information.)

To transfer the data to the DVD-RAM or USB flash memory drive:

1. Select a CPC (server).
2. Open **Save Legacy Upgrade Data**. The Save Legacy Upgrade Data window is displayed.
3. Depending on the CPC you chose, insert the Support Element's Upgrade Data DVD-RAM or USB flash memory drive. The Select Media Device window is displayed.
4. Select the media that you want to transfer data to, then click **OK**.
5. A message window is displayed indicating the success of failure of the operation.

Use the online Help if you need additional information for saving legacy upgrade data.

Single Step Internal Code Changes



Notes:

- Before starting this task, make sure you have a formatted USB flash memory drive (with volume label of **ACTBKP**) available for backing up critical data. (See "USB flash memory drive" on page 10 for more information.)
- Single Step Internal Code Changes is considered a disruptive task. If the object is locked, you must unlock it before continuing. For more information about disruptive tasks, see "Disruptive tasks" on page 6.

This task allows you to retrieve and apply, apply only, or remove licensed internal code for one or more objects.

You can do any of the following:

- Choose to only apply internal code changes or to retrieve and apply internal code changes.
- Determine if pending internal code changes are disruptive. If so, you can choose to activate the changes concurrently or disruptively.
- Verify the system environment. In the case of a Support Element, it verifies that the most recent Alternate Support Element mirroring operation was successful and that a Service Required state does not exist.
- Perform a Backup Critical Data function.
- Accept all previously activated internal code changes (optional).
- Retrieve internal code changes from the IBM Service Support System.
- Connect to the IBM Service Support System and download any internal code change *hold* status for pending internal code changes.
- Connect to IBM Service Support System to see if the status of any existing internal code changes has changed from non-disruptive to disruptive.
- Install and activate the internal code changes.
- Choose to retrieve and apply (or clone) internal code changes to match a saved clonable level.
- Choose to receive all code changes for your system regardless of the requirements for installing the next Engineering Change (EC) level.
- Trigger the Alternate Support Element mirroring operation.
- Transmit system availability data to the remote support system.

Certain licensed internal code changes may require the MRU to shut down during the activation of the change. This is normal for these changes. This could cause a slight degradation in system performance during the time the MRU is shut down. After activation is complete, the MRU will be turned on again, and normal performance will be resumed.

To retrieve, apply, or remove licensed internal code:

1. Select one or more CPCs (servers).
2. Open the **Single Step Internal Code Changes** task. The Apply Single Step Internal Code Changes window is displayed.
3. Verify the objects that are listed and review the **Single Step Code Change Overview** information. If you want to proceed with the actions/defaults described in that window, click **Retrieve and Install...** to start the operation. Otherwise, if you have additional options that you want to perform for this task, click **Advanced...**
4. Follow the instructions on the subsequent windows to complete the task, or click **Cancel** to end the task.

This task also allows you to retrieve and apply a previous saved level of internal code (clonable) from the IBM Service Support System. Before continuing with this task, you must have a saved level of internal code stored in the IBM Service Support System. For more information for creating a clonable level of internal code, see the **Define Clonable Internal Code Levels** task in the *Support Element Operations Guide*.

To retrieve and apply internal code changes to a Support Element to match a saved clonable level:

1. Select a CPC (server).
2. Open the **Single Step Internal Code Changes** task. The Apply Single Step Internal Code Changes window is displayed.
3. To access additional options, click **Advanced...**, the Apply Single Step Internal Code Changes window is displayed which includes additional options.
4. Select **Retrieve and apply (Clone) internal code changes to match a saved clonable level**, then click **OK**. The Retrieve Clonable Level Data window is displayed.
5. Specify the *serial number* of the Support Element where the internal code was saved from in the **Machine Serial Number** input field.
6. Specify the *name* that you gave to the clonable level of internal code in the **Clonable Level Name** input field.
7. Specify the *password* that you defined for this clonable level of internal code in the **Clonable Level Password** input field, then select **Retrieve Clonable Level Data**. The Single Step Internal Code Changes Apply Busy window is displayed while the system is retrieving the data from the IBM Service Support System.
8. Select **Apply Concurrent Internal Code Changes**. The Single Step Internal Code Changes Progress window is displayed. Wait for the task to complete; otherwise, follow the instructions on the subsequent windows.

Use the online Help to get additional information on working with an internal code change.

Special Code Load



Notes:

- You cannot perform this task remotely.

- Special Code Load is considered a disruptive task. If the object is locked, you must unlock it before continuing. For more information about disruptive tasks, see “Disruptive tasks” on page 6.

This task is used when you want to preload a new CPC internal code level on the alternate Support Element while the remainder of the system is running.

To upgrade to Version Code 1.6.0 or later:

1. Select one or more CPCs (servers).
2. Open the **Special Code Load** task. The Confirm the Action window is displayed.
3. Install the Support Element microcode (CD-ROM) in the Hardware Management Console CD-ROM drive and click **OK**. Follow the rest of the directions shipped with your upgrade package.

Use the online Help if you need additional information for upgrading to the new Version Code.

System Information



This task displays information about a selected CPC (server) and its licensed internal code. 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 IBM product engineering. 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 the system information:

1. Select one or more CPCs (servers).
2. Open the **System Information** task. The System Information window is displayed.
3. Select the internal code information you want to view.
 - To view the additional information about this internal code, click **EC Details...**
 - To display information about further actions that may need to be taken, click **Query Additional Actions...**

Note: This option is available only if the selected CPC is at Version 2.10.0 or later.

4. Click **OK** when you have completed this task.

Use the online Help if you need additional information about internal code change information.

Remote Customization



Remote Customization tasks customize the remote capabilities of the CPC Support Elements in the processor cluster.

The following tasks are represented in the *Remote Customization* task group:

- Customer Information
- Remote Service
- Support Element Operations Guide

Customer Information



This task enables you to customize the customer information for a CPC or a group of CPCs.

To customize your customer information:

1. Select one or more CPCs (servers).
2. Open the **Customer Information** task. The Customer Information window is displayed
3. Select one of the following tabs from the Customer Information window:
 - Administrator
 - System
 - Account
4. Supply the appropriate 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 the information that applies to the first selected object. The information for the other objects will be displayed by tabs on the right.
5. Click **OK** when you have completed the task.

Use the online Help if you need additional information for customizing a CPC's account information.

Remote Service



This task allows you to enable or disable remote service for individual objects or a group of objects. When enabled, error information may be sent by a Hardware Management Console operator or automatically to IBM for analysis and for service call requests. When disabled, error information and requests for service must be done through voice communications.

Authorize automatic service call reporting will send error information and requests for service automatically to IBM without operator intervention.

To customize remote service settings:

1. Select one or more objects (servers).

2. Open the **Remote Service** task. The Remote Service Configuration window is displayed.
 - Enable remote service by selecting **Enable remote service requests**. This option (a check mark is displayed) allows the Hardware Management Console to establish remote connections for the object or objects to your service provider's remote service support system.
 - Enable automatic service calling by selecting:
 - **System z** to set the console to automatically report System z problems and request service.
 - **zBX** to set the console to automatically report IBM zEnterprise BladeCenter Extension (zBX) problems and request service.

Note: This option is available only when the zBX feature is installed. For additional zBX information, see the *Hardware Management Console Operations Guide for Ensembles*.
3. Verify the **Customer Service Center Telephone Number** is correct or provide a new one in the input area.
4. Click **OK** when you have completed the task.

Use the online Help if you need additional information about remote service for an object.

Support Element Operations Guide



This task allows you to view the online publication for the CPC you are currently working with.

Note: If you are accessing the Hardware Management Console remotely, a PDF version of the document is available. If you are accessing the Hardware Management Console locally, an HTML version of the document is available for System z10 and later.

To the display the *Support Element Operations Guide*:

1. Select a CPC (server).
2. Open the **Support Element Operations Guide** task. The *Support Element Operations Guide* publication, that is applicable for the CPC you are working with, is displayed.
3. When you have finished viewing the publication, click the **X** in the upper right corner of the window to close the book.

Use the online Help if you need additional information for displaying the *Support Element Operations Guide*.

Operational Customization



Operational Customization tasks are used to display or modify the profiles that make the CPCs operational, set the date and time for automatic licensed internal code to be updated, and set the date and time on the Support Element(s).

The following tasks are represented in the *Operational Customization* task group:

- Automatic Activation
- Change LPAR Controls
- Change LPAR Group Controls
- Change LPAR I/O Priority Queuing
- Configure Channel Path On/Off
- Customize/Delete Activation Profiles
- Customize Scheduled Operations
- Customize Support Element Date/Time
- Enable I/O Priority Queuing
- Logical Processor Add
- OSA Advanced Facilities
- Reassign Channel Path
- View Activation Profiles

Automatic Activation



This task controls whether the selected CPC is activated automatically when power is restored following a utility power failure. Follow your local procedures for recovering from a power outage that is the result of a utility power failure. You may, however, be able to speed recovery from such power outages by enabling *Automatic Activation* for the selected CPC.

- When automatic activation is *enabled* and a utility power failure occurs, the CPC is activated automatically when the 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* (default setting) and a utility power failure occurs, the CPC power remains off when the power is restored. You can activate the CPC manually at any time once the utility power is restored. If the system had been IMLed without using **Activate**, then the CPC is not automatically activated when power is restored, even if automatic activation is enabled.

To enable or disable automatic activation:

1. Select one or more CPCs (servers).
2. Open the **Automatic Activation** task. The Automatic Activation window is displayed.
3. Click **Enable** or **Disable** depending on your preference.
4. Click **Save** to save the setting and close the window.

Use the online Help if you need additional information about automatic activation.

Change LPAR Controls



This task allows you to review or change logical processor assignments of logical partitions and the CPC's settings for processor running time if the selected CPC is operating in logically partitioned (LPAR) mode.

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 only to the logical partition. 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, and the processing weights 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. Normally after the CPC is activated, changing its control settings requires opening and customizing a reset profile and then using the profile to activate the CPC again. Likewise, after the CPC is activated in LPAR mode, changing the control settings of its logical partition requires opening and customizing their image profile and then using the profile to activate the logical partition. Through this task you can change some of the control settings *dynamically* (new settings take affect without customizing profiles or activating objects).

To change control settings of the CPC and the logical partitions that can be activated on it:

1. Select a CPC (server).
2. Open the **Change LPAR Controls** task. The Change Logical Partition Controls window is displayed.
3. Depending on the physical processors installed in your system (CPs, ICFs, IFLs, IFAs, 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.

From this window you have the option to export the data table to a Comma Separated Values (csv) file for audit purposes as well as performing further analysis. If you are accessing the Hardware Management Console remotely you can click **Export** to perform this function.

4. Select the **Processor Running Time** tab to change the control settings of the logical partitions, then proceed to indicate what you want to do with the new settings.

Use the online Help to get additional information about changing LPAR controls.

Change LPAR Group Controls



This task allows you to view or change a group assignment for logical partitions. It displays the group name, member partitions, and group capacity value that can be customized in determining the allocation and management of processor resources assigned to the group. It also allows changing a group assignment dynamically for active logical partitions.

To change LPAR group controls:

1. Select a CPC (server).
2. Open the **Change LPAR Group Controls** task. The Change LPAR Group Controls window is displayed.
3. You can click **Edit** on the menu bar to change the group capacity value and the group members.
4. Once you have made your changes to those windows you can either:
 - Click **Save to Profiles** if you want the new settings to take effect whenever the selected CPC and its logical partitions are activated with the modified profiles,
 - Click **Change Running System** if you want the new settings to take effect immediately, or
 - Click **Save and Change** if you want the new settings to take effect immediately and whenever the selected CPC and its logical partitions are activated with the modified profiles.

Use the online Help to get additional information for changing LPAR group controls.

Change LPAR I/O Priority Queuing



This task allows you to review or change the minimum or maximum 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 values.

To change LPAR I/O priority queuing:

1. Select one or more CPCs (servers).
2. Open the **LPAR I/O Priority Queuing** task. The Change Logical Partition Input/Output (I/O) Priority Queuing window is displayed.
3. The window lists the I/O priority queuing values for logical partitions defined by this IOCDS.
4. Use the window to dynamically change the minimum and maximum values.

Note: If global 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**.

5. Make a selection to indicate what you want to do with the new setting.

Use the online Help to get additional information for changing LPAR I/O priority queuing.

Configure Channel Path On/Off



Notes:

- Configure Channel Path On/Off is considered a disruptive task. If the object is locked, you must unlock it before continuing. For more information about disruptive tasks, see “Disruptive tasks” on page 6.
- Depending on your user task role, you may only be able to view this task.

This task configures channel paths on and off. *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 the Hardware Management Console workplace to configure channel paths on and 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 shared 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 operating system facilities rather than the Hardware Management Console workplace, whenever possible, to configure channel paths on and off.

To use the workplace to configure channel paths on or off:

1. Select a CPC image.
2. Open the **Configure Channel Path On/Off** task. The Disruptive Task Confirmation window is displayed. Since this task may be disruptive to the targeted CPC image, review the confirmation text in the window to decide whether or not to proceed with the task.
3. If you proceed with the task, the Configure Channel Path On/Off window is displayed.
4. The window displays the *current state* and *desired state* of each channel path.
5. Use the window list and actions to *toggle* the desired states of channel paths you want to configure on or off.
6. Click **Apply** to make the desired states take effect.

Use the online Help to get additional information for configuring channel paths.

Customize/Delete Activation Profiles



This task enables you to create new activation profiles, customize existing profiles, or delete unwanted profiles that are stored in the Support Element. An activation profile is required for CPC or image activation and defines the IOCDS, storage sizes, and other parameters that will be available when the object is activated.

Note: Depending on your user task role, you may only be able to view this task.

The *DEFAULT RESET*, *DEFAULT IMAGE*, and *DEFAULT GROUP* profiles are the only profiles that can use the same name. For more information about activation profiles, see the **Customize/Delete Activation Profiles** task in the *Support Element Operations Guide*.

To create new, customize existing, or delete activation profiles:

1. Select one or more objects.
2. Open the **Customize/Delete Activation Profiles** task. The Customize/Delete Activation Profiles List window is displayed.
3. If you selected more than one object for this task, then tabs on the right side of the window allow you to work with the objects you selected.
4. Select a profile from the list, then click an action you want to perform, such as **Customize selected profile**. The Customize Activation Profiles window is displayed. This window uses a tree view to present the activation profile information.

The tree view located on the left side of the window includes the CPC that you want to work with and its images, if applicable. You can expand on each of these items by clicking on the square and you can then click on each name for more details or to make appropriate changes to the profile.

You can also use the **Image Profile Wizard** to modify parameters of image profiles. From the Customize/Delete Activation Profiles List window:

1. Select the profile name that requires modification, then click **Image profile wizard**. The Select one or more images window is displayed.
2. Select one or more profiles to modify, then click **OK**. The Image Wizard window is displayed.
3. Proceed through the wizard windows propagating the desired information.
4. Click **Finish** when you have completed the task and are ready to save the changes.

Use the online Help to get additional information for working with profiles and see the **Customize/Delete Activation Profiles** task in the *Support Element Operations Guide*.

Customize Scheduled Operations



This task allows you to schedule the times and dates for automatic licensed machine code updates and backup of critical hard disk data for one or more CPC Support Elements. Calling customize scheduled operations displays all scheduled operations, their scheduled dates and times, the functions, and the numbers of repetitions.

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).

The operations that can be scheduled on a Hardware Management Console are:

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.

Backup critical hard disk information

Schedules an operation to make a backup of critical hard disk information for the selected CPCs.

Accept internal code changes

Schedules an operation to make activated internal code changes a permanent working part of the licensed internal code of selected CPCs.

Install and activate concurrent code changes

Schedules an operation for installing and activating internal code changes retrieved for the selected CPCs.

Remove and activate concurrent code changes

Schedules an operation for removing and activating internal code changes installed for the selected CPCs.

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 selected CPC

Schedules an operation for activating a selected CPC.

Deactivate (Power off) selected CPC

Stops the operating system, deallocates resources, clears associated hardware and powers off the CPC.

Access external time source

Schedules an operation to obtain data from an external time source by dialing out to the Hardware Management Console for the purpose of synchronizing the time of the selected servers (CPCs) that are participating in a Server Time Protocol (STP) Coordinated Timing Network (CTN).

Transmit system availability data

Sends service data generated by the selected object to IBM. This data is used to ensure a high level of availability.

Change LPAR weights

Schedules an operation to change the processing weight for processor types assigned to one or more active logical partitions and allows the partition capping value to be specified. Specify only the weights for active partitions that you want to change or that you want to be active. If a partition specified does not exist or is not active at the time the operation runs, then the entire scheduled operation is ignored. This operation is available only for a System z10 at Version 2.10.1 or later.

Audit and Log Management

Schedules an operation to generate an audit report on selected types of audit data.

To schedule any of the previous operations:

1. Select one or more CPCs (servers).
2. Open the **Customize Scheduled Operations** task. The Customize Scheduled Operations window is displayed.
 - To add a scheduled operation, point to **Options** from the menu bar, then click **New...** The Add a Scheduled Operation window is displayed. From this window select an operation that you want performed and select an object to perform if you targeted more than one CPC for this task, then click **OK**. The Set up a Scheduled Operation window is displayed. In this window select the date and time for the operation to occur and whether or not it repeats, then click **Save**.
 - To delete a scheduled operation, select the operation you want to delete, point to **Options** from the menu bar, then click **Delete**. The Confirm the action window is displayed, click **OK** to remove the scheduled operation.

- To view a scheduled operation, select the operation you want to view, point to **View** from the menu bar, then click **Schedule Details...** The Details window is displayed.
 - To change the time of a scheduled operation, select the operation, point to **View** from the menu bar, then click **New Time Range...** The Change the Time Range window is displayed.
 - To sort the scheduled operations, point to **Sort** from the menu bar, then click one of the sort groups that appear.
3. To return to the Hardware Management Console workplace, point to **Options** from the menu bar, then click **Exit**.

Use the online Help to get additional information for scheduling operations.

Customize Support Element Date/Time



This task enables you to update the date and time of the Support Element of a single CPC, multiple CPCs, or a group of CPCs that are defined to this Hardware Management Console. The updated date and time can be the date and time that is currently set for the Hardware Management Console or it can be a date and time that you enter.

Notes:

- A CPC that is synchronized to a time source using either the External Time Reference (ETR) feature or the Server Time Protocol (STP) feature cannot have its date and time customized with this task. However, this task will cause the Support Element to synchronize its time to the time source.
- Depending on your machine type and model the Support Element **Clock** and **Time zone** fields cannot be modified by the Hardware Management Console. In that case, you must use the **Single Object Operations** task to set the Support Element clock and time zone.

For a procedure on changing the Support Element date and time, see Appendix F, “Changing your time-of-day clock,” on page 239. You can also use the online Help if you need additional information.

Enable I/O Priority Queuing



This task allows you to enable or disable global input/output (I/O) priority queuing for the system. Enabling I/O priority queuing allows the 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 query decisions with multiple requests.

To enable I/O priority queuing:

1. Select one or more CPCs (servers).
2. Open the **Enable I/O Priority Queuing** task. The Enable I/O Priority Queuing window is displayed.
3. Click the drop-down menu under **Setting** to make your selection for the specified CPCs:

Enabled

Activates I/O priority queuing for the CPC.

Disabled

Deactivates I/O priority queuing for the CPC.

4. Click **Save** to save the setting.

Use the online Help to get additional information for enabling I/O priority queuing.

Logical Processor Add

This task 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 “Customize/Delete Activation Profiles” on page 174 for more information.

To dynamically add one or more logical processors:

1. Select a CPC image.
2. Open the **Logical Processor Add** task for an active partition. The Logical Processor Add window is displayed.
3. Based on the current logical partition configuration, change the logical processor definitions for the partition:
 - a. Increase the initial values, reserved values, or both for installed logical processor types.
 - b. 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.
 - c. Increase the reserved value for logical processor types that have not been installed and already have reserved CPs defined.
4. To have the new changes take effect immediately, click **Change Running System**.

Use the online Help if you need additional information for adding one or more logical processors or initially setting logical processor values.

OSA Advanced Facilities

The Open Systems Adapter (OSA) is an integrated hardware feature plug-in as a channel card, becoming an integral component of the I/O subsystem, enabling convenient Local Area Network (LAN) attachment. This brings the strengths of the architecture to the client/server environment: security, availability, enterprise-wide access to data, and systems management.

Note: Depending on your user task role, you may only be able to view this task.

You can use the Hardware Management Console workplace to open a facility for monitoring, operating, and customizing an OSA channel.

To work with an OSA channel:

1. Select a CPC (server).
2. Open the **OSA Advanced Facilities** task. The OSA Advanced Facilities window is displayed.

3. If this window lists channels that are not available because they are offline, click **OK**; this displays the next OSA Advanced Facilities window.
4. Click the channel ID with which you want to work and then click **OK**. This displays the Advanced Facilities window.
5. Click the function of your choice:

View code level

Displays the channel ID, channel type, and code level for the card.

Card trace/log/dump facilities...

Selects any of the following actions:

- Display or alter trace mask
- Read trace buffer
- Read log buffer

Card specific advanced facilities...

Performs any of the following actions:

- Enable or disable ports
- Query port status
- Run port diagnosis
- View port parameters
- View code level
- Display or alter MAC address
- 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.

OSA reset to defaults...

Resets OSA to the default configuration.

Then click **OK**.

6. The next window that displays depends on your selection.
 - 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 OSA Reset to Default Configuration window, click **Yes** to reset OSA to the default configuration.

Use the online Help to get additional information for working with OSA Advanced Facilities.

Reassign Channel Path



Reassign is a channel operation you can use to perform at once all the following steps necessary to reassign a reconfigurable channel path from its owning logical partition to another logical partition:

- Configuring off the channel path from its owning logical partition, if necessary.
- Releasing the channel path, if necessary.
- Configuring on the channel path to the other logical partition.

To reassign a channel path:

1. Select a CPC (server).
2. Open the **Reassign Channel Path** task, the Reassign Channel Path window is displayed.
3. In the list, select the channel path identifier that you want to reassign, then click **Reassign**. The Select a Partition window is displayed showing the channel path that is currently assigned, the owning partition, and a list of logical partitions from which you can select to reassign the channel path.
4. Select the logical partition in the **Target Partition** list to which you want the channel path reassigned, then click **Reassign**. The Confirm the Action window is displayed.
5. Click **Reassign** to confirm your request to reassign the selected channel path to the target logical partition.

Note: You may receive an additional warning that the channel 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 **Release and Reassign** to confirm the action.

6. After the channel path is reassigned, click **OK** to close the window.

Use the online Help if additional information is needed for reassigning a channel path.

View Activation Profiles



This task enables you to view the activation profiles that are stored in the CPC Support Element.

To view the activation profile:

1. Select one or more objects (CPCs or CPC images).
2. Open the **View Activation Profiles** task. The View Activation Profiles List window is displayed.
3. Select a profile name to view the activation profile information, then click **View**. The View Load Profiles window is displayed.
4. When you are done reviewing this information, click **Cancel** to go back to the previous window.

Use the online Help to get additional information for viewing an activation profile.

Object Definition



This task is used to define the objects (CPCs, ESCON Directors, Sysplex Timers, or Fiber Savers) that will be available to the Hardware Management Console. A server (CPC) must be defined to a Hardware Management Console before other tasks can be performed on the server (CPC).

If the undefined server (CPC) *can* be automatically discovered by the Hardware Management Console, the CPC is displayed in the **Undefined CPCs** work area if you are using the classic interface or under **Unmanaged Resources>Servers** in the navigation pane using the tree interface when the Hardware Management Console is powered on. To define the server (CPC), use the **Add Object Definition** task.

If the undefined CPC *cannot* be automatically discovered by the Hardware Management Console, the CPC will not appear in the undefined CPCs group when the Hardware Management Console is powered on. To define the CPC, see “Add Object Definition” to manually add an object.

Note: When using either interface the CPC groups are referred to as *defined CPCs* or *undefined CPCs*.

The following tasks are represented in the *Object Definition* task group:

- Add Object Definition
- Change Object Definition
- Reboot Support Element
- Remove Object Definition

Add Object Definition



Notes:

- An object with a domain name that is different from the domain name of the Hardware Management Console will not communicate with the Hardware Management Console or appear on any of the Hardware Management Console windows.
- This task will not be successful if a mirroring operation is in progress.

This task enables you to define a server (CPC) that is currently not defined and was automatically discovered by the Hardware Management Console. After a CPC is defined it becomes part of the **Defined CPCs** in the classic interface or it is part of **Servers** in the tree interface. Each object must have a unique name and TCP/IP address.

You can also use this task to define an ESCON Director console, Sysplex Timer console, or Fiber Saver that is currently not defined.

To add a CPC, ESCON Director, Sysplex Timer, or Fiber Saver to a defined group:

1. Select an undefined object.
2. Open the **Add Object Definition** task under the **Object Definition** task list. The Add or Change Object window is displayed.
3. Click **Save** to add the object to your group of defined objects.

You can also use this task to provide the additional addressing information to configure Support Elements to remote Hardware Management Consoles. At the remote Hardware Management Console:

1. Open the **Undefined CPCs** group (classic interface) or **Unmanaged Resources>Servers** (tree interface).
2. Select **CPC Manual Definition**. (See “CPC Manual Definition” on page 64 for more information.)
3. Open the **Add Object Definition** task under **Object Definition** task list. The Manual Add Object Definition window is displayed.
4. Specify the TCP/IP address in the **Addressing Information** field and click **OK**. The Hardware Management Console tries to contact the Support Element and exchange the remaining information necessary to complete the configuration process.

Note: The Manual Add Object Definition window remains displayed with the last entered TCP/IP address until you have added the appropriate CPCs. When you have completed this task, click **Cancel**.

5. All objects that you added will appear in the **Defined CPCs** group (classic interface) or **Servers** group (tree interface).

Use the online Help to get additional information for adding servers (CPCs).

Change Object Definition



Note: Alternate Support Element must be operational and not mirroring to allow change.

This task enables you to change the definition of any object that is defined. After the change is complete, the object's definition will be changed in all groups that contain the object. Each object must have a unique name and TCP/IP address.

To change a CPC, ESCON Director, Sysplex Timer, or Fiber Saver:

1. Select a defined object.
2. Open the **Change Object Definition** task under the **Object Definition** task list. The Add or Change Object window is displayed.
3. Make any necessary changes to the object, click **Save** to save the changes for the object.

Use the online Help to get additional information for changing a server (CPC) name.

Reboot Support Element



Note: Reboot Support Element is considered a disruptive task. If the object is locked, you must unlock it before continuing. For more information about disruptive tasks, see “Disruptive tasks” on page 6.

This task allows you to reboot the Support Element of the selected server (CPC) without logging on at the actual Support Element console. Use this task if you are currently operating from a remote location and the Support Element is not easily accessible. An example of when you would want to reboot the Support Element from the Hardware Management Console is after a change has been made to the TCP/IP configuration of the Support Element.

To reboot the Support Element:

1. Select one or more CPCs (servers).
2. Open the **Reboot Support Element** task. The Reboot Support Element Task Confirmation window is displayed.
3. Click **Yes** to continue with this task, or click **No** to exit the task.

Use the online Help if additional information is needed for rebooting the Support Element.

Remove Object Definition



This task, used by an access administrator or a user ID that is assigned access administrator roles, enables you to remove a server (CPC) that is currently part of the **Defined CPCs** group in the classic style user interface or **Servers** in the navigation pane for the tree style user interface. During definition removal, the Remove Object Definition Task Confirmation window is displayed, if the option was set on the User Settings Confirmations page, to allow you to continue or quit the **Remove Object Definition** task.

After a CPC is removed from the **Defined CPCs** or **Servers** group, it is added to the **Undefined CPCs** or **Unmanaged Resources** group. No further action will be possible on that server (CPC) from the Hardware Management Console that removed its definition, status will not be reported, and messages will not be available.

To remove an object:

1. Select an object.
2. Open the **Remove Object Definition** task. The Remove Object Definition Task Confirmation window is displayed.
3. Click **Yes** to continue with this task, or click **No** to exit the task.

Use the online Help to get additional information for deleting a defined server (CPC).

Configuration



Configuration tasks are used to display, transmit, or update the configuration files kept for the CPCs.

The following tasks are represented in the *Configuration* task group:

- Edit Frame Layout
- Input/Output (I/O) Configuration Save and Restore
- System Input/Output Configuration Analyzer
- System (Sysplex) Time
- Transmit Vital Product Data
- View Frame Layout

Edit Frame Layout



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. Select an object.
2. 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.

3. Click **Save** when you have completed the task and want to save your changes.

Use the online Help if you need additional information for adding, moving, or removing devices and adding frames.

Input/Output (I/O) Configuration Save and Restore



This task allows you to save, restore, or erase Input/Output (I/O) configuration data files for a specified object on the Hardware Management Console.

Note: If you choose to save data files on the Hardware Management Console, any previously saved files will be erased.

To save or restore data files:

1. Select a CPC (server).
2. Open the **Input/Output Configuration Save and Restore** task. The Input/Output Configuration Save and Restore window is displayed.
3. Select one of the options:
 - Save data files
 - Restore data files
 - Restore only the IOCDS data files
 - Restore only the channel configuration files
 - Erase the data files
4. Click **OK** to proceed with your choice, or click **Cancel** to exit the task.

Use the online Help if you need additional information on saving or restoring I/O configuration data files.

System Input/Output Configuration Analyzer



This task is used to analyze and help you manage your current System Input/Output Configuration (SIOC). The data can be viewed in several different arrangements giving emphasis to one item. You can filter the data and it will be applied to all applicable views. You can also 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.

To analyze this information:

1. Select a CPC (server).
2. Open the **System Input/Output Configuration Analyzer** task. The System Input/Output Configuration Analyzer window is displayed. Initially, the PCHID Control Unit View window displays the current I/O configuration data by the PCHID control unit.

A menu bar is displayed at the top of the window with the following options:

- Select **File** to:
 - Save Data to USB Flash Memory Drive (This option is available only if you are accessing the Hardware Management Console locally.)
Insert a USB flash memory drive so the data can be copied (see “USB flash memory drive” on page 10 for more information). A progress window is displayed when the operation has completed.
 - Refresh
 - Exit
- Select **View** to display the following types of information you want displayed in the table:
 - PCHID Control Unit
 - PCHID Partition
 - Control Unit
 - Link Load
 - Node ID
- Select **Filter** to display a smaller, narrowed down version of the information in the table you are working with. Some of the filter options may include:
 - PCHID
 - CSS.CHPID
 - Switch
 - Partition

- Control Unit
 - Show All
 - Select **Sort** to arrange the data in the table in descending or ascending order depending on the parameters you specified.
3. When you have finished reviewing this information, select **File** from the menu bar, then **Exit** to end the task and return to the Hardware Management Console workplace.

Use the online Help if you need additional information on analyzing the SIOC information.

System (Sysplex) Time



Note: System (Sysplex) Time is considered a disruptive task. If the object is locked, you must unlock it before continuing. For more information about disruptive tasks, see “Disruptive tasks” on page 6.

This task allows you to view or setup time synchronization for a server (CPC) using the Sysplex Timer or Server Time Protocol (STP). A *Sysplex Timer* is a device that provides a time source to the time-of-day (TOD) clocks of Central Processor Complexes (CPCs) attached to it and the operating systems or control programs running that server (CPC). *Server Time Protocol* (STP) is a time synchronization architecture designed to provide the capability for multiple servers (CPCs) to maintain time synchronization with each other and to form a Coordinated Timing Network (CTN).

See Appendix E, “Using the System (Sysplex) Time task,” on page 229 for more detailed information and procedures on using this task. You can also use the online Help if you need additional information to complete this task.

Transmit Vital Product Data



This task provides a window for you to collect Vital Product Data (VPD) from the Support Element of all CPCs that are defined to your Hardware Management Console and to either transmit the data to the IBM Service Support System or to store the information on diskette (if one is available), USB flash memory drive, or Hardware Management Console hard disk.

To send vital product data from the Support Element to the Hardware Management Console:

1. Select one or more CPCs (servers).
2. Open the **Transmit Vital Product Data** task. The Transmit Vital Product Data to IBM window is displayed.
3. Select the type of vital product data you want to transmit from the Transmit Vital Product Data to IBM window:
 - System (Support Element) vital data
 - Hardware Management Console vital product data
4. Select the destination to which you want to transmit:
 - IBM service support system
 - Diskette (if one is available)
 - USB flash memory drive (see “USB flash memory drive” on page 10 for more information)
 - Hardware Management Console hard disk

and then click **OK** to proceed.

Use the online Help if you need additional information for transmitting VPD data.

View Frame Layout



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. Select a CPC (server).
2. 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.

3. Click **OK** when you are done viewing the frame layout.

Use the online Help to get additional information for viewing the physical location of objects defined to the Hardware Management Console.

Energy Management



Energy Management tasks are used to provide power and thermal monitoring capability and controls for the CPCs.

The following tasks are represented in the *Energy Management* task group:

- Set Power Cap
- Set Power Saving

For more detailed information on the energy management tasks, see the *Hardware Management Console Operations Guide for Ensembles*.

Set Power Cap



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. Select a CPC (server), BladeCenter, or individual blade.
2. 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 CPC.
3. Specify the power capping setting in the **Power Capping Setting** list.
4. Specify the power cap in the **Cap Value** field.
5. Click **OK** to complete the task.

Use the online Help if you need additional information about setting the power cap.

Set Power Saving



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.

To set power saving:

1. Select a CPC (server), BladeCenter, or individual blade.
2. Open the **Set Power Saving** task. The Set Power Saving window is displayed. The window lists the current power saving settings for the CPC.
3. Specify the power saving setting for the CPC resources in the **Power Saving** list

Level 01a

4. Click **OK** to complete the task.

Use the online Help if you need additional information about setting power saving.

Monitor



Monitor tasks are used to monitor the selected CPCs.

The following tasks are represented in the **Monitor** task group:

- Environmental Efficiency Statistics
- Monitors Dashboard (includes the Customize Activity Profiles and Activity tasks)
- Monitor System Events

Environmental Efficiency Statistics



Note: This task can only be used with a zEnterprise System CPC.

This task allows you to display environmental efficiency data graphically and in table format for the selected CPC. Environmental efficiency data that displays includes the following:

- Power consumption (kW and Btu)
- Temperature (Celsius and Fahrenheit)
- CP utilization percentage

Note: In addition to CPs; ICFs, IFLs, zIIPs, and zAAPs are also included in this measurement.

- Blade CPU utilization percentage

To display environmental efficiency statistics data:

1. Select a CPC.
2. Open the **Environmental Efficiency Statistics** task. The Environmental Efficiency Statistics window is displayed.
3. Specify a start date and make a selection from the duration list.
4. Click **Refresh** to update the window.
5. From the Chart Content list select the graphical display that you prefer.
6. If you are accessing the Hardware Management Console remotely, click **Export** to save the environmental efficiency data that is currently displayed to a Comma Separated Values (csv) file.
7. When you have completed this task, click **Close**.

Use the online Help to get additional information on displaying environmental efficiency data.

Monitors Dashboard



Note: This task can only be used with a zEnterprise System CPC.

Use this task to monitor system activity and display activity details on your system for the selected CPCs.

To monitor system activity for your system:

1. Select one or more CPCs.

2. Open the **Monitors Dashboard** task. The **Monitors Dashboard** window is displayed. The overview table includes information on processor and channel usage, power consumption, and ambient air temperature. Expand the Details section to view activity details for the CPCs.
3. To display summaries of processing and channel activity for the selected CPC, expand the Details section for the CPCs you want to monitor. Refer to “Activity” for more information.
4. To work with system activity profiles, select **Open Activity Profiles** located above the Overview table. The Customize Activity Profiles window for the selected CPC is displayed. Refer to “Customize Activity Profiles” on page 192 for more information.
5. When you have finished viewing this information, click **Close**.

Use the online Help to get additional information about monitoring your system.

Activity

The **Open Activity** selection from the **Monitors Dashboard** task displays the system activity for CPCs or a group of CPCs. System activity includes the channel activity and physical processing activity that has been defined in the system activity profiles that are stored in the selected CPCs. For more information about assigning and customizing activity profiles for CPCs, see “Customize Activity Profiles” on page 192.

Available screen space and resources provide a practical upper limit on the number of System Activity displays that can be active at one time. Starting the **Activity** task when another instance of the task is already running does not stop the previous task instance.

Note: The utilization reported by the **Activity** task for most channel types will agree with the utilization reported by Resource Measurement Facility™ (RMF™). For fiber channels, however, this task considers the channel to be busy any time an operation is pending, even if the channel is waiting for a device to respond. Whereas, RMF looks at the amount of work done versus the amount of work that could be done by the channel. This means that if you have devices that are relatively slow to respond, leaving the channel waiting for a response but otherwise idle, **Activity** will show a utilization that is significantly higher than that reported by RMF.

To display system activity:

1. Select **Open Activity** located above the Overview table.
 - If you select a single object for the task, both the System Activity Summary window is displayed and the System Activity window is displayed.

The System Activity Summary window displays the system activity for each object on a single line. The activity displayed as a blue bar is the average of all reported physical processor processing activity for the CPC. The activity displayed as a green bar is the average of all reported channel activity for the CPC. One or both types of activities can be displayed for the selected objects. A red bar indicates that activity data is not available for the object. You can choose different variations of the information to be displayed:

 - Both processor and channel activity in graphics (this is the default view)
 - Processor activity only in graphics
 - Both processor and channel activity in text
 - Channel activity only in graphics.

The System Activity window displays more detailed information about the processing or channel activity as a percentage. It changes as the amount of activity changes. It can also optionally show the power being consumed and the air input temperature for those systems that support it. You can use the **Font Size** arrows to increase or decrease the size font for the information being displayed.
 - If you selected more than one object, the System Activity Summary window is displayed. You can then double-click on a summary bar for that object to display its System Activity details window.
2. When you are done reviewing the system activity details, click the red **X** in the upper right corner of the window to close the task window.

Use the online Help to get additional information on monitoring system activity.

Customize Activity Profiles



The **Open Activity Profiles** selection from the **Monitors Dashboard** task displays the system activity profiles for the objects you have selected and performs actions on the profiles. You can view an existing profile, make changes to it, delete it, or change the status. You can also specify which profiles are used in the **Activity** task for reporting activity on objects on the Hardware Management Console.

To work with system activity profiles:

1. Select one or more objects (servers).
2. Select **Open Activity Profiles** located above the Overview table. If you selected a single object, the Customize Activity Profiles for ... window is displayed. If you selected multiple objects, the Customize System Activity Profile List window is displayed and there are tabs on the right indicating the object names that you selected. You can click on the individual tabs to go to the profile list for each object.
3. Select a profile name then choose an action:
 - Click **Customize** to change the system activity profile for the selected object. The Customize System Activity Profile window is displayed. You can make appropriate changes, then click **Save** to save the changed information.
 - Click **Delete** to remove the selected system activity profile name from the object.
 - Click **Change Status** to change the status of the selected system activity profile name.
 - Click **Reset** to discard the changes you made and return to the options when you opened the task.
4. To exit the task without making any changes, click **Cancel**.

Use the online Help to get additional information for working with a object's activity profile.

Monitor System Events



This task allows you to create and manage event monitors. Event monitors listen for state changes events from the virtual machines the Hardware Management Console manages.

When an event is received, the monitor tests it with user-defined time and text filters. If the event passes the tests, the monitor sends email to interested users. The **Monitor System Events** task allows you to enable or disable monitors and display or change information about settings such as the SMTP port.

An event monitor has the following characteristics:

- Unique name on the Hardware Management Console
- Persistent
- Enabled or disabled without changing its other characteristics
- Listens to one or more managed objects
- Notifies users by email if an event is received from a managed object and it passes through all the filters of the event monitor
- Contains a regular expression filter that must match the event text for the monitor to notify users
- Limited by time filters, such:
 - A set of days, for example, Monday through Friday

- A range of times during the day, for example 8 a.m. through 4 p.m.
- A range of dates, for example, 2/14/2005 to 2/16/2005.

To create or change an event monitor:

1. Select a virtual machine from the **Managed z/VM Virtual Machines Work Area** in the classic interface or from the **All z/VM Virtual Machines** group in the tree interface.
2. Open the **Monitor System Events** task. The Event Monitor Summary window is displayed.
3. View or change **Settings** information:
 - SMTP server
 - SMTP port
 - Minimum time between emails.
4. To create an event monitor, select the **State Change Example** monitor and click **Add...** to create a state change event monitor. (z/VM virtual machines only support state change events.) The Event Monitor Editor window is displayed. Provide the appropriate information in the input fields. Ensure that you select the virtual machines whose state you want to monitor in the list of objects to be monitored. Click **OK** to finish creating the event monitor.

To edit an existing monitor, select the monitor from the monitor list on the Event Monitor Summary window then click **Edit...** to edit that monitor.

5. To test an event monitor for the specified SMTP server, click **Test....**
6. Click **OK** from the Event Monitor Summary window when you have completed this task.

Use the online Help if you need additional information about creating and managing event monitors or see “Monitor System Events” on page 112.

z/VM Virtual Machine Management



z/VM Virtual Machine Management tasks are used to manage z/VM virtual machines from the Hardware Management Console. This task group is displayed only if one or more server images are running z/VM V5.3 or later. Accessing these tasks require a user ID with system programmer roles.

The following tasks are represented in the *z/VM Virtual Machine Management* task group:

- Activate
- Choose z/VM Virtual Machines to Manage
- Deactivate
- Edit the VMRM Active Configuration File
- Grouping
- Maintain z/VM Profiles
- Maintain z/VM Prototypes
- Maintain z/VM Virtual Machines to Manage
- Maintain z/VM Volume Space
- Undefine z/VM Virtual Machines for Management
- View the VMRM Measurement Data
- z/VM Virtual Network Information

Note: If you are using the tree interface the **Activate**, **Deactivate**, and **Grouping** tasks appear under the **Daily** task group.

Activate



This task controls starting up the virtual machine and performing the initial program load of the virtual machine operating system software. Activate is your primary function for virtual machine start up. Activate senses the status of the object and does not perform the activation if the virtual machine is already active.

To start activation of a z/VM virtual machine:

1. Select one or more virtual machines from the **Managed z/VM Virtual Machines Work Area** in the classic interface or from the **All z/VM Virtual Machines** group in the tree interface.
2. Open the **Activate** task under **z/VM Virtual Machine Management** in the classic interface or under **Daily** in the tree interface. The Activate Task Confirmation window is displayed.

Note: Activation profiles are not applicable for virtual machines.

3. If you want to continue this task, click **Yes**. If you want to end the task, click **No**. If you click **Yes**, the Activate Progress window is displayed indicating the progress of the activation and the outcome.
4. 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.

Choose z/VM Virtual Machines to Manage



Note: You can manage only z/VM virtual machines for server images that meet the following conditions:

- Server image is running z/VM V5.3 or later.
- Hardware Management Console is at Version 2.9.2 or later.
- Support Element is at Version 1.8.2 or later and has the necessary code updates that allows for communications with z/VM.

This task chooses the virtual machines from the server image that are to be managed by the Hardware Management Console.

1. Select a server image that is running z/VM V5.3 or later.
2. Open the **Choose z/VM Virtual Machines to Manage** task. The Choose z/VM Virtual Machines to Manage window is displayed which includes a list of virtual machine IDs.
3. From the list, select the virtual machine IDs that you want to manage from the Hardware Management Console.
4. Click **OK** to proceed. The configured virtual machines are included in the Managed z/VM Virtual Machines group in the classic interface or in the **All z/VM Virtual Machines** custom group in the tree interface.

You can also use this task to undefine the virtual machines the Hardware Management Console is managing.

1. Select a server image that is running z/VM V5.3 or later.
2. Open the **Choose z/VM Virtual Machines to Manage** task. The Choose z/VM Virtual Machines to Manage window is displayed which includes a list of virtual machine IDs.
3. From the list, clear the virtual machine ID that you no longer want to manage from the Hardware Management Console.
4. Click **OK** to proceed. The virtual machines are no longer included in the **Managed z/VM Virtual Machines** group in the classic interface or in the **All z/VM Virtual Machines** custom group in the tree interface.

Use the online Help for more information about configuring virtual machines.

Deactivate



This task stops the virtual machine and the virtual machine operating system software.

To start deactivation of a z/VM virtual machine:

1. Select one or more virtual machines from the **Managed z/VM Virtual Machines Work Area** in the classic interface or from the **All z/VM Virtual Machines** group in the tree interface.
2. Open the **Deactivate** task under **z/VM Virtual Machine Management** in the classic interface or under **Daily** in the tree interface. The Deactivate Task Confirmation window is displayed.
3. Review the information about the window to verify that the object (or objects) you deactivate is the correct one. If you want to continue this task, click **Yes**. If you want to end the task, click **No**. If you click **Yes**, the Deactivate Progress window is displayed indicating the progress of the deactivation and the outcome.

- 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.

Edit the VMRM Active Configuration File



Note: You can manage only z/VM virtual machines for server images that meet the following conditions:

- Server image is running z/VM V5.4.
- Hardware Management Console is at Version 2.10.1 or later.
- Support Element is at Version 1.8.2 or later and has the necessary code updates that allows for communications with z/VM.

This task updates the Virtual Machine Resource Manager (VMRM) configuration file. This task invokes an editor where you can update the file and the data is temporarily saved on the Hardware Management Console.

1. Select a CPC (server) image that is running z/VM V5.4.
2. Open the **Edit the VMRM Active Configuration File** task. The Edit the VMRM active Configuration File window is displayed.
3. Click **Yes** to proceed with editing the configuration file. Otherwise, click **No** to cancel the task.
4. If you proceed to edit the configuration file, an editor is invoked where you can update the VMRM configuration file. The changes are temporarily saved on the Hardware Management Console, however, you can continue with one of the following options:
 - Syntax check the VMRM configuration data and optionally save the data to z/VM.
 - Syntax check the VMRM configuration data and save the data to z/VM.
 - Cancel the changes to end the task.

Note: Using this interface, the default name and location must be used. The configuration file is saved as VMRM CONFIG VMSYS:VMRMSVM.

Grouping



This task enables you to create, delete, add to, or delete from user-defined groups of objects. When you select one or more virtual machines and open the **Grouping** task, the Manage Groups window is displayed, allowing you to specify what type of action you want to take on the group. You might want to create a group when you want to perform the same task on several virtual machines simultaneously instead of repeating the task on each individual virtual machine.

To group z/VM virtual machines:

1. Select one or more virtual machines from the **Managed z/VM Virtual Machines Work Area** in the classic interface or from the **All z/VM Virtual Machines** group in the tree interface.
2. Open the **Grouping** task under **z/VM Virtual Machine Management** in the classic interface or under **Daily** in the tree interface.
3. The Manage Groups window is displayed allowing you to add the selected object (or objects) to an existing group, remove the selected object from a group, create a group, create a pattern match group, remove the group, create a pattern match group, or edit an existing pattern match group. Click **OK** to proceed with your selections.

You can also create a *Pattern Match* group. A *Pattern Match* group is a group that contains all virtual machines of a given type whose names match a certain pattern (for example, all virtual machines starting with P0).

To create a group with all z/VM virtual machines starting with P0:

1. Select the object (or objects) you want to work with, then open the **Grouping** task. The Manage Groups window is displayed. Select **Create a new pattern match group** on the Manage Groups window, then click **OK**. The Create Pattern Match Group window is displayed.
Or, you can open the **Grouping** task without selecting an object. The Create Pattern Match Group window is displayed.
2. Specify *P0.** in the **Managed Resource Pattern** field on the Create Pattern Match Group window as shown in Figure 51.
3. Specify *P0group* in the **New group name** field, provide a description in the **New group description** input field, and select **z/VM Virtual Machines** as the Group type, then click **OK**.
4. You receive a message that the group (*P0group*) has been created and the selected objects have been added to it.

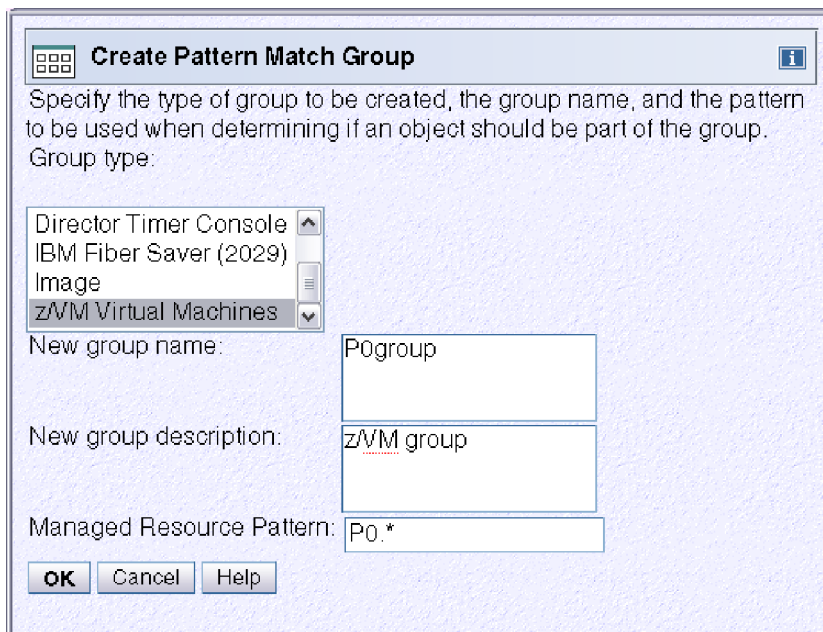


Figure 51. Create pattern match group window for virtual machines

Any new groups that you create are displayed in the **Groups Work Area** for the classic interface and in **Custom Groups** for the tree interface. Also, an entry is displayed in the **Customize User Controls** task in the Manage Resource Roles table that indicates a group has been added. The entry is **Groups created by *userid***, where *userid* is the name of the user that created the group.

This task also allows you to group one or more user-defined groups into other groups. 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.

Use the online Help if you need additional information for working with groups and see “Grouping” on page 139.

Maintain z/VM Profiles



Note: You can manage only z/VM profiles for server images that meet the following conditions:

- Server image is running z/VM V5.4.
- Hardware Management Console is at Version 2.9.2 or later.
- Support Element is at Version 1.8.2 or later and has the necessary code updates that allows for communications with z/VM.

This task allows you to add a new z/VM profile or specify a z/VM profile to view, change, remove, lock, or unlock.

1. Select a server image that is running z/VM V5.4.
2. Open the **Maintain z/VM Profiles** task. The Maintain z/VM Profiles window is displayed.
3. Proceed with any of the following options:
 - Click **Add...** to add a new profile, the Add a New z/VM Profile window is displayed. Specify a new profile name in the **Virtual Machine Profile Name** entry field (make note of the new profile name that you are adding) and specify directory statements in the **Directory Statements** field.
 - Specify a profile name and click **View...** to view an existing profile, the View an Existing z/VM Profile window is displayed.
 - Specify a profile name and click **Change...** to change an existing profile, the Change an Existing z/VM Profile window is displayed.
 - Specify a profile name and click **Remove** to remove an existing profile.
 - Specify a profile name and click **Lock** to lock an existing profile.
 - Specify a profile name and click **Unlock** to unlock an existing profile.
4. When you are ready to exit the task, click **Cancel**.

Use the online Help for more information about maintaining the z/VM profiles.

Maintain z/VM Prototypes



Note: You can manage only z/VM prototypes for server images that meet the following conditions:

- Server image is running z/VM V5.3 or later and has a directory manager installed.
- For profile support, the server image is running z/VM V5.4.
- Hardware Management Console is at Version 2.9.2 or later.
- Support Element is at Version 1.8.2 or later and has the necessary code updates that allows for communications with z/VM.

This task allows you to add a new z/VM prototype or to select an existing z/VM prototype to view, change, or remove.

1. Select a server image that is running z/VM V5.3 or later and has a directory manager installed.
2. Open the **Maintain z/VM Prototypes** task. The Maintain z/VM Profiles window is displayed. Proceed with any of the following options:
 - Click **Add...** to add a new prototype, the Add a New z/VM Prototype window is displayed.
 - Click **View...** to view a selected prototype, the View an Existing z/VM Prototype window is displayed.

- Click **Change...** to change a selected prototype, the Change an Existing z/VM Prototype window is displayed.
 - Click **Remove** to remove a selected prototype.
3. When you are ready to exit the task, click **Cancel**.

Use the online Help for more information about maintaining the z/VM prototypes.

Maintain z/VM Virtual Machines to Manage



Note: You can maintain only z/VM virtual machines for server images that meet the following conditions:

- Server image is running z/VM V5.3 or later and has a directory manager installed.
- For profile support, the server image is running z/VM V5.4.
- Hardware Management Console is at Version 2.10.1 or later.
- Support Element is at Version 1.8.2 or later and has the necessary code updates that allows for communications with z/VM.

This task allows you to add a new z/VM virtual machine or to select a z/VM virtual machine to view, change, remove, lock, unlock, or maintain disks for.

1. Select a server image that is running z/VM V5.3 or later and has a directory manager installed.
2. Open the **Maintain z/VM Virtual Machines to Manage** task. The Maintain z/VM Virtual Machines to Manage window is displayed.

Proceed with any of the following options:

- Click **Add...** to add a new virtual machine, the Add a New z/VM Virtual Machine window is displayed.
 - Click **View...** to view a selected virtual machine, the View an Existing z/VM Virtual Machine window is displayed.
 - Click **Change...** to change a selected virtual machine, the Change an Existing z/VM Virtual Machine window is displayed.
 - Click **Remove...** to remove a selected virtual machine, the Remove an Existing z/VM Virtual Machine window is displayed.
 - Click **Lock...** to lock a selected virtual machine, the Lock a z/VM Virtual Machine window is displayed.
 - Click **Unlock...** to unlock a selected virtual machine, the Unlock a z/VM Virtual Machine window is displayed.
 - Click **Maintain Disks...** to maintain disk for a selected virtual machine, the Maintain Disks for an Existing z/VM Virtual Machine window is displayed.
3. When you are ready to exit the task, click **Cancel**.

Use the online Help for more information about maintaining the z/VM virtual machines.

Maintain z/VM Volume Space



Note: You can manage only z/VM volume space for server images that meet the following conditions:

- Server image is running z/VM V5.3 or later and has a directory manager installed.
- For profile support, the server image is running z/VM V5.4.

- Hardware Management Console is at Version 2.10.1 or later.
- Support Element is at Version 1.8.2 or later and has the necessary code updates that allows for communications with z/VM.

This task allows you to maintain z/VM volume space by querying, defining, or removing volume space.

1. Select a server image that is running z/VM V5.3 or later and has a directory manager installed.
2. Open the **Maintain z/VM Volume Space** task. The Maintain z/VM Volume Space window is displayed. This window displays the results of an initial default query to display all the volume definitions.

Proceed with any of the following options:

- Click **Query** to run another volume space query based on the values you specified.
 - Click **Define...** to define volume space to the directory manager, the Define Volume Space to the Directory Manager window is displayed.
 - Click **Remove...** to remove the directory manager, the Remove Volume Space to the Directory Manager window is displayed.
3. When you are ready to exit the task, click **Cancel**.

Use the online Help for more information about maintaining the z/VM volume space.

Undefine z/VM Virtual Machines for Management



This task is used when the selected virtual machine does not need to be managed by the Hardware Management Console.

1. Select one or more virtual machines from the **Managed z/VM Virtual Machines Work Area** in the classic interface or from the **All z/VM Virtual Machines** group in the tree interface.
2. Open the **Undefine z/VM Virtual Machines for Management** task. The Undefine z/VM Virtual Machines for Management Task Confirmation window is displayed.
3. Verify that the selected virtual machines in the Object Names list are the ones you no longer want managed by the Hardware Management Console.
4. Click **Yes** to proceed with the task.

Use the online Help if you need additional information about the confirmation window.

View the VMRM Measurement Data



Note: You can manage only z/VM virtual machines for server images that meet the following conditions:

- Server image is running z/VM V5.3 or later.
- Hardware Management Console is at Version 2.10.1 or later.
- Support Element is at Version 1.8.2 or later and has the necessary code updates that allows for communications with z/VM.

This task allows you to view the Virtual Machine Resource Manager (VMRM) measurement data.

1. Select a server image that is running z/VM V5.3 or later.

2. Open the **View the VMRM Measurement Data** task. The View VMRM Measurement Data window is displayed. This window displays the file name of the active configuration file, the time stamp of the active configuration file, and the timestamp from the z/VM system when the VMRM measurement data was taken.
3. When you have reviewed the information and are ready to exit this task, click **Cancel**.

Use the online Help for more information on viewing the VMRM measurement data.

z/VM Virtual Network Information



This task allows you to view detailed information about the virtual networks and switches for the selected z/VM image.

1. Select a CPC image that is running z/VM V5.3 or later.
2. Open the **z/VM Virtual Network Information** task. The Virtual Network Information window is displayed.
3. You can select the **Guest LAN** tab for information about all guest virtual LAN segments defined for the z/VM image.
4. You can select the **Virtual Switch** tab for information about all virtual network switches defined for the z/VM image.
5. Click **Cancel** when you have finished viewing this information.

Use the online Help if you need more detailed information about the virtual network information.

Appendix A. Tasks and default user IDs

This appendix lists the tasks you can perform using the Hardware Management Console and the predefined default user IDs that are initially associated with that task. You can, however, create customized user profiles which would allow you to have unique user IDs and multiple user roles. The management of these user roles is performed by using the **Customize User Controls** task. The **User Profiles** task provides the ability to define which user roles are to be associated with each specific user ID.

Table 2 lists the tasks that can be performed on the console and the corresponding predefined default user IDs that can perform these tasks.

Table 3 on page 205 lists the tasks that can be performed on the objects and the corresponding predefined default user IDs that can perform these tasks.

Note: For tasks that are assigned the Ensemble Administrator (ENSADMIN) or Ensemble Operator (ENSOPERATOR) default user IDs see the *Hardware Management Console Operations Guide for Ensembles*.

Table 2. Hardware Management Console tasks and default user IDs

Tasks	Default user IDs				
	OPERATOR	ADVANCED	SYSPROG	ACSADMIN	SERVICE
Analyze Console Internal Code					X
Archive Security Logs			X	X	X
Audit and Log Management			X	X	X
Authorize Internal Code Changes			X		X
Backup Critical Console Data			X		X
Block Automatic Licensed Internal Code Change Installation				X	
Certificate Management			X	X	X
Change Console Internal Code		X	X		X
Change Password	X	X	X	X	X
Configure 3270 Emulators			X		
Configure Data Replication				X	
Console Default User Settings				X	
Console Messenger	X	X	X	X	X
Copy Console Logs to Media					X
Create Welcome Text				X	
Customize API Settings			X	X	
Customize Auto Answer Settings		X	X	X	X
Customize Automatic Logon				X	
Customize Console Date/Time	X	X	X	X	X
Customize Console Services			X	X	X
Customize Customer Information			X		X
Customize Modem Settings			X		X
Customize Network Settings				X	X

Table 2. Hardware Management Console tasks and default user IDs (continued)

Tasks	Default user IDs				
	OPERATOR	ADVANCED	SYSPROG	ACSADMIN	SERVICE
Customize Outbound Connectivity			X		X
Customize Product Engineering Access				X	
Customize Remote Service			X		X
Customize Scheduled Operations			X		X
Customize User Controls				X	
Domain Security				X	X
Enable Electronic Service Agent				X	
Enable FTP Access to Mass Storage Media			X		
Fibre Channel Analyzer	X	X	X	X	X
Format Media	X	X	X	X	X
Hardware Management Console Settings		X	X	X	X
Installation Complete Report					X
Logoff or Disconnect	X	X	X	X	X
Manage Enterprise Directory Server Definitions				X	
Manage Print Screen Files	X	X	X	X	X
Manage Remote Connections	X	X	X	X	X
Manage Remote Support Requests	X	X	X	X	X
Manage SSH Keys				X	X
Manage Users Wizard				X	
Manage Web Services API Logs			X	X	
Monitor System Events			X		
Network Diagnostic Information	X	X	X	X	X
Object Locking Settings		X	X	X	X
Offload Virtual RETAIN Data to Removable Media	X	X	X	X	X
Password Profiles				X	
Perform a Console Repair Action					X
Reassign Hardware Management Console					X
Rebuild Vital Product Data					X
Remote Hardware Management Console	X	X	X	X	X
Report a Problem	X	X	X		X
Restore Legacy HMC Data					X
Save/Restore Customizable Console Data				X	
Save Upgrade Data					X
Shutdown or Restart	X	X	X	X	X
Single Step Console Internal Code		X	X		X
Tip of the Day	X	X	X	X	X
Transmit Console Service Data	X	X	X	X	X

Table 2. Hardware Management Console tasks and default user IDs (continued)

Tasks	Default user IDs				
	OPERATOR	ADVANCED	SYSPROG	ACSADMIN	SERVICE
Transmit Vital Product Data			X		X
User Patterns				X	
User Profiles				X	
User Settings	X	X	X	X	X
User Templates				X	
Users and Tasks	X	X	X	X	X
View Console Events	X	X	X	X	X
View Console Information	X	X	X	X	X
View Console Service History	X	X	X	X	X
View Console Tasks Performed					X
View Licenses	X	X	X	X	X
View PMV Records	X	X	X	X	X
View Security Logs			X	X	X
What's New	X	X	X	X	X

Table 3. Tasks performed on objects and default user IDs

Tasks	Default user IDs				
	OPERATOR	ADVANCED	SYSPROG	ACSADMIN	SERVICE
Hardware Messages	X	X	X	X	X
Operating System Messages	X	X	X	X	X
Daily					
Activate	X	X	X		X
Deactivate	X	X	X		X
Grouping			X	X	
Reset Normal	X	X	X		X
Recovery					
Access Removable Media			X		X
Integrated 3270 Console	X	X	X		X
Integrated ASCII Console	X	X	X		X
Load	X	X	X		X
Load from Removable Media or Server			X		X
PSW Restart		X	X		X
Reset Clear	X	X	X		X
Reset Normal	X	X	X		X
Single Object Operations	X	X	X	X	X
Start All		X	X		X
Stop All		X	X		X
Service					
Archive Security Logs			X		X

Table 3. Tasks performed on objects and default user IDs (continued)

Tasks	Default user IDs				
	OPERATOR	ADVANCED	SYSPROG	ACADMIN	SERVICE
Backup Critical Data			X		X
Perform Problem Analysis	X	X	X		X
Perform Transfer Rate Test					X
Report a Problem	X	X	X		X
Restore Critical Data					X
Service Status	X	X	X	X	X
Transmit Service Data	X	X	X	X	X
View PVM Records	X	X	X	X	X
View Service History	X	X	X		X
Change Management					
Alternate Support Element			X		X
Alternate Support Element Engineering Change (ECs)					X
Change Internal Code		X	X		X
Concurrent Upgrade Engineering Changes (EC)			X		X
Engineering Changes (ECs)					X
Product Engineering Directed Changes					X
Retrieve Internal Code		X	X		X
Save Legacy Upgrade Data					X
Single Step Internal Code Changes		X	X		X
Special Code Load					X
System Information	X	X	X	X	X
Remote Customization					
Customer Information			X		X
Remote Service			X		X
Support Element Operations Guide	X	X	X	X	X
Operational Customization					
Automatic Activation			X		
Change LPAR Controls			X		X
Change LPAR Group Controls			X		X
Change LPAR I/O Priority Queuing			X		X
Configure Channel Path On/Off		X	X		
Customize/Delete Activation Profiles			X		
Customize Scheduled Operations			X		X
Customize Support Element Date/Time	X	X	X	X	X
Enable I/O Priority Queuing			X		X
Logical Processor Add			X		X
OSA Advanced Facilities			X		X

Table 3. Tasks performed on objects and default user IDs (continued)

Tasks	Default user IDs				
	OPERATOR	ADVANCED	SYSPROG	ACADMIN	SERVICE
Reassign Channel Path		X	X		X
View Activation Profiles	X	X			X
Object Definition					
Add Object Definition				X	X
Change Object Definition				X	X
Reboot Support Element				X	X
Remove Object Definition				X	
Configuration					
Edit Frame Layout					X
Input/Output (I/O) Configuration Save and Restore					X
System Input/Output Configuration Analyzer			X		X
System (Sysplex) Time			X		X
Transmit Vital Product Data			X		X
View Frame Layout			X		
Energy Management					
Set Power Cap			X		X
Set Power Setting			X		X
Monitor					
Environmental Efficiency Statistics	X	X	X		X
Monitors Dashboard	X	X	X	X	X
Monitor System Events			X		
z/VM Virtual Machine Management					
Activate			X		
Choose z/VM Virtual Machines to Manage			X		
Deactivate			X		
Edit the VMRM Active Measurement Data			X		
Grouping			X		
Maintain z/VM Profiles			X		
Maintain z/VM Prototypes			X		
Maintain z/VM Virtual Machines			X		
Maintain z/VM Volume Space			X		
Undefine z/VM Virtual Machines for Management			X		
View the VMRM Measurement Data			X		
z/VM Virtual Network Information			X		

Appendix B. Enhanced driver maintenance

This appendix discusses the Concurrent Upgrade Engineering Changes (CUEC) feature that eliminates the need for downtime when you are adding new functions. You can upgrade the firmware engineering change (EC) drivers to the next EC level without any performance impact during an upgrade. A system outage is no longer required in order to take advantage of most, if not all, new enhancements. Enhanced driver maintenance is performed by your IBM Service Support System.

Switch points

The firmware components include:

- Support Element (SE)
- Flexible Service Processor (FSP)
- Power
- LPAR
- Coupling Facility Control Code (CFCC)
- i390 / Millicode
- Channels.

Each of these firmware components has its own EC stream to release code fixes and new functions to the field.

When CUEC is used to upgrade the firmware, the driver GA^n to driver GA^{n+1} has designated switch points. This means that each GA^n firmware EC stream must be at a specified internal code change level, and the initial CUEC activation can only transition to a specified internal code change level for each GA^{n+1} EC stream.

Not every fix bundle supports CUEC. Therefore, as part of the fix-apply process, your operator must make a decision whether to apply internal code changes above a CUEC switch point. You must develop a plan that indicates when to use CUEC to go to the next GA level and map this plan to an IBM published plan for CUEC switch point release dates (refer to Resource Link at <http://www.ibm.com/servers/resourcelink>). If another scheduled CUEC switch point release is shown to be prior to your targeted GA upgrade date, you can apply fixes above the current CUEC switch point. However, if no additional CUEC switch point releases are planned before the GA upgrade target, your operator should not apply internal code changes above the current CUEC switch point.

Note: It is not recommended to remove fixes in order to get back to a CUEC switch point.

Concurrent Upgrade Engineering Changes (EC) task

Use the **Concurrent Upgrade Engineering Changes (EC)** task to take you through the proper steps for a successful CUEC.

1. Select the CPC you are updating.
2. Open the **Concurrent Upgrade Engineering Changes (EC)** task. The Concurrent Upgrade Engineering Changes window is displayed as shown in Figure 52 on page 210.

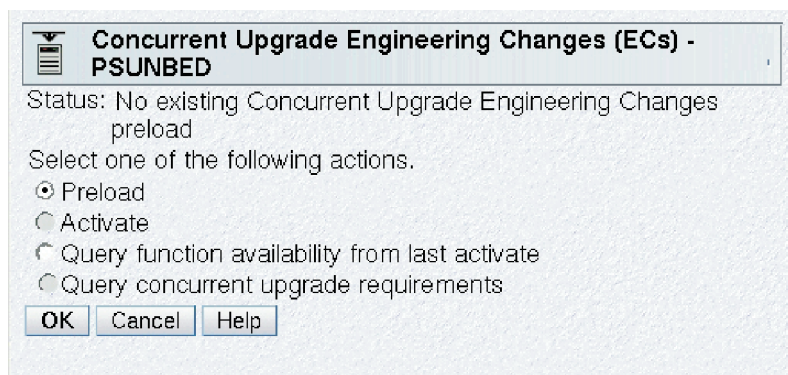


Figure 52. Concurrent upgrade engineering changes (ECs) task window

3. Choose the action to perform in the order as it is displayed (refer to the appropriate sections for more information):
 - “Preload”
 - “Activate” on page 211
 - “Query function availability from last activate” on page 213 (recommended).
4. Click **OK** to proceed.

Preload

The **Preload** action is the first step in the CUEC process to initially preload the alternate SE with the GAⁿ⁺¹ code while the primary SE and the system continue to operate using the GAⁿ code.

From the Concurrent Upgrade Engineering Changes (EC) window:

1. Select **Preload** to load engineering changes in order to upgrade the CPC to a new level. (This option is available only if your user ID is assigned the service representative task role.)
2. The Preload Options window is displayed as shown in Figure 53.

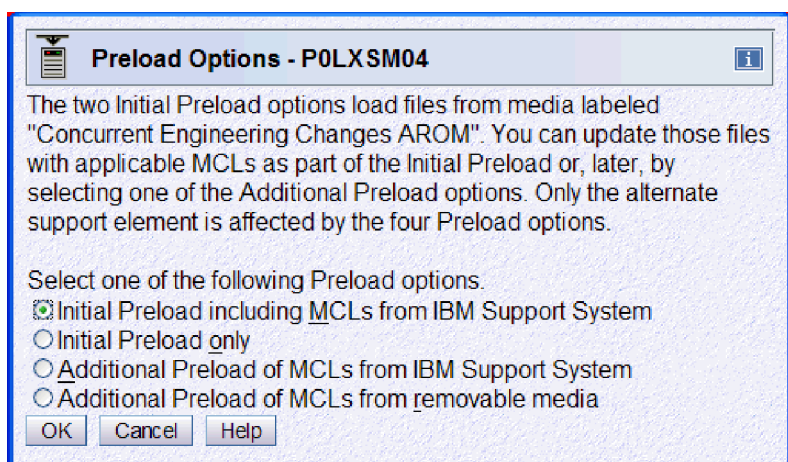


Figure 53. Preload options

3. Choose an option, then click **OK** to proceed.

Initial preload options

The **Initial Preload** options put the base GAⁿ⁺¹ driver on the alternate SE using the CUEC AROM. Choose one of the **Initial Preload** options:

- **Initial Preload including MCLs from IBM Support System** – upgrades the CPC to a new level and then automatically retrieves and installs all applicable internal code changes from the IBM Service Support System.
- **Initial Preload only** – upgrades the CPC to a new level without retrieving related internal code changes.

The only difference in these two options is that the first option downloads any additional fixes that were released after that CUEC AROM was released.

When one of the initial preload options is selected, the HMC validates that the CUEC AROM appropriately matches the from- GA^n system EC. Then, a check is made to ensure that the CUEC GA^n switch point requirements are met. If CUEC minimum internal code change requirements are not satisfied, but no CUEC maximum requirement has been exceeded, the operator is given the option to concurrently apply additional GA^n internal code changes in order to meet the CUEC requirements. If at least one CUEC maximum internal code change requirement has been exceeded, the operator is told that the CUEC is not possible. It is not recommended to remove fixes. You must wait for the next CUEC switch point.

Once the validation process has successfully completed, the Hardware Management Console triggers the download of the new GA^{n+1} code onto the alternate SE. Configuration and customization data are preserved during this transition from GA^n to GA^{n+1} code.

Finally, if the CUEC initial preload option included the request to retrieve internal code changes, the alternate SE would retrieve from the IBM Service Support System any additional internal code changes that were not part of the CUEC AROM. These additional internal code changes would be applied on the alternate SE hard disk following certain defined restrictions because the CUEC activation process must concurrently manage the firmware updates in memory where that firmware executes.

Additional preload options

The **Additional Preload** options can be executed only after the initial preload has been performed. These options allow the download of additional fixes that were not part of the initial preload step.

- **Additional Preload of MCLs from IBM Support System** – retrieves and installs all applicable internal code changes from the IBM Service Support System.
- **Additional Preload of MCLs from removable media** – retrieves and installs all applicable internal code changes from removable media. The removable media is displayed as **Mass Readable Media Device** on the Select Media Device window. This type of media device can be a CD-ROM, DVD-RAM, or USB flash memory drive whose capacity is 1 GB or greater. (See “USB flash memory drive” on page 10 for more information.)

Activate

The **Activate** option is the second step of the CUEC process.

From the Concurrent Upgrade Engineering Changes (EC) window:

1. Select **Activate** as shown in Figure 54 on page 212. (This option is available only if your user ID is assigned the service representative task role.)

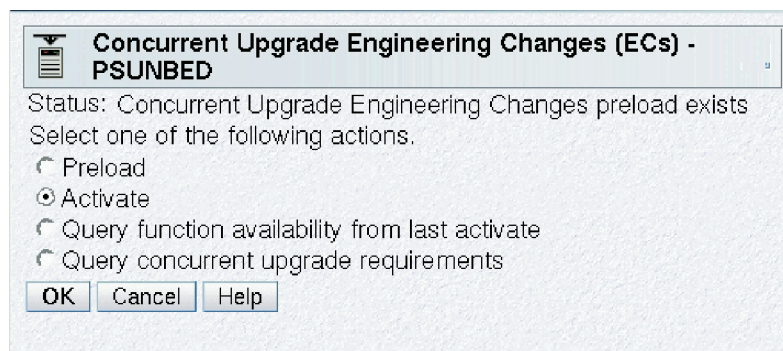


Figure 54. Activate option

2. Then click **OK** to proceed.
3. The following three phases are part of the activation process before the activation of the upgrade is complete:
 - a. "Preparation"
 - b. "Transition"
 - c. "Completion."

The following three phases are included for the activation of the upgrade.

Preparation

The preparation phase makes sure that the following requirements are verified before the code switch starts:

- The concurrent patch feature is enabled.
- The CUEC GA^n switch point requirements are met (if the internal code changes applied to the GA^n code on the primary SE changed since the CUEC preload).
- No pending conditions from previous CUEC or concurrent patch sessions exist.
- There is enough free memory for the additional GA^{n+1} HSA. The driver information contains the CUEC GA^{n+1} memory requirements. If there is not enough memory, then you are told how much memory to free. You must provide memory by deactivating a partition or varying off storage in a partition if the complete memory is used.

Transition

The transition phase is the heart of the CUEC activate because it is in this step that the GA^{n+1} code is applied in each firmware subsystem memory. The Support Element (SE) is the first subsystem to have its GA^{n+1} code loaded and this is done by executing a CUEC alternate SE switch. This causes the GA^{n+1} code to become the new primary SE while the GA^n code becomes the new alternate SE. The GA^{n+1} new primary SE must restart and perform a warm-start resynchronization with the other firmware subsystems. Once the primary SE completes its warm-start synchronization, it serially triggers each of the subsystems to load its GA^{n+1} firmware.

Completion

The completion phase includes a hardware message that could be displayed directing the operator to invoke two tasks to complete the GA^{n+1} transition from those exception firmware subsystems.

- **Query Channel/Crypto Configure Off/On Pending** - this task allows the operator to see which channels and cryptos must be configured offline and put back online in order to get the GA^{n+1} code loaded.
- **Query Coupling Facility Reactivations** - this task informs the operator whether any coupling facility (CF) partitions must be reactivated in order to move the CFCC code for that partition to GA^{n+1} .

Query function availability from last activate

Once the CUEC activate is complete the final step of the CUEC process is performed.

From the Concurrent Upgrade Engineering Changes (EC) window:

1. Select **Query function availability from last activate**, then click **OK**.
2. The Query Function Availability from Last Activate window is displayed. A list of functions which are not yet available or have not yet been enabled after the CUEC process completed is displayed in the window.

or

A message window is displayed, indicating that all functions are enabled and available.

This option addresses the exception cases where one or more new GA^{n+1} functions cannot be made available during the CUEC activation process. Some possible reasons why these functions are not available include:

- Not all subsystems have moved to the GA^{n+1} code level. The operator can use the **Query Channel/Crypto Configure Off/On Pending** and **Query Coupling Facility Reactivations** Support Element tasks to ensure that the GA^{n+1} code level transitions have completed. Once this GA^{n+1} code level validation is completed, the operator can invoke the **Query Function Availability from Last Activate** option to see what functions are still not available.
- One or more exception functions might require some additional action to finalize the enablement/availability for those functions. This could include an action such as configuring off/on for certain types of channel or processors.

Refer to the appropriate *System Overview* publication and to Resource Link (<http://www.ibm.com/servers/resourcelink>) for descriptions of the new functions available for the GA^{n+1} release. They can also inform you of any additional actions required to fully enable/make available any functions that can be displayed on the **Query Function Availability from Last Activate** window.

Completing the upgrade

Once you have permanently moved to the GA^{n+1} level on the primary system you need to bring the alternate system to the GA^{n+1} level. To accomplish this upgrade, proceed with the following:

1. Use the **Backup Critical Data** task on the GA^{n+1} system.
2. Using the CUEC AROMs, perform a hard disk restore on the GA^n system.
3. From the **Restore Critical Data** window, select the backup file needed to restore the critical data, then click **OK**.

Appendix C. Remote operations

Remote operations are designed for human interaction and use the Graphical User Interface (GUI) used by a local Hardware Management Console operator. There are two ways to perform operations remotely (see Figure 55):

- Use a remote Hardware Management Console, or
- Use a web browser to connect to a local Hardware Management Console.

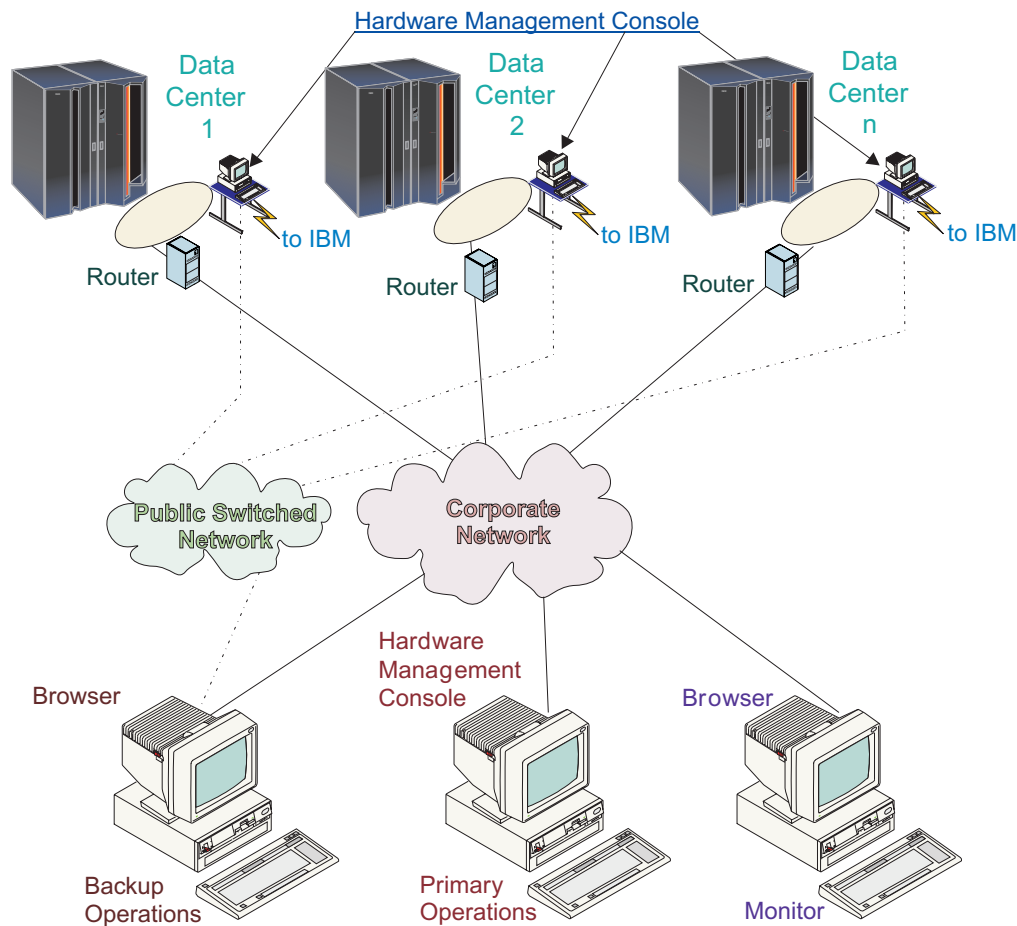


Figure 55. Remote operation configuration

The *remote Hardware Management Console* is a Hardware Management Console that is on a different subnet from the Support Element, therefore the Support Element cannot be autodiscovered with IP multicast.

The choice between a remote Hardware Management Console and a web browser connected to a local Hardware Management Console is governed principally by the scope of control that is needed. A remote Hardware Management Console defines a specific set of managed objects that is directly controlled by the remote Hardware Management Console, while a web browser to a local Hardware Management Console has control over the same set of managed objects as the local Hardware Management Console. The communications connectivity and communication speed is an additional consideration; LAN connectivity provides acceptable communications for either a remote Hardware Management Console or web browser control, but dial-up connectivity only works with web browser control; a remote Hardware Management Console cannot connect using dial-up connections.

Using a remote Hardware Management Console

A remote Hardware Management Console gives the most complete set of functions because it is a complete Hardware Management Console; only the process of configuring the managed objects is different from a local Hardware Management Console (see “Add Object Definition” on page 181). As a complete Hardware Management Console, a remote Hardware Management Console has the same setup and maintenance requirements as a local Hardware Management Console. A remote Hardware Management Console needs LAN TCP/IP connectivity to each managed object (Support Element) that is to be managed; therefore, any customer firewall that may exist between the remote Hardware Management Console and its managed objects must permit Hardware Management Console to Support Element communications to occur. A remote Hardware Management Console may also need communication with another Hardware Management Console for service and support. Table 4 shows the ports a remote Hardware Management Console uses for communications.

Table 4. Ports used by a remote Hardware Management Console for communications

Port	Use
tcp 443	Single Object Operations to Support Element and remote browser access
tcp 25345	Single Object Operations to legacy Support Element
tcp 55555	Hardware Management Console to Support Element commands
tcp 58787	Hardware Management Console to Support Element discovery
udp 9900	Hardware Management Console to Hardware Management Console discovery
tcp 9920	Hardware Management Console to Hardware Management Console commands
ICMP Type 8	Ping to/from Support Element to Hardware Management Console
tcp 4455	Director/Timer communications
tcp 21	Only when Electronic Service Agent or Enable FTP Access to Hardware Management Console Mass Storage Media need to be used

A remote Hardware Management Console needs connectivity to IBM (or another Hardware Management Console that has connectivity to IBM) for service and support. The connectivity to IBM may be in the form of access to the internet (through a company firewall), or a dialed connection through a customer provided switched phone connection using the supplied modem (see “Customize Outbound Connectivity” on page 97). A remote Hardware Management Console cannot use the supplied modem for communication with a local Hardware Management Console or a Support Element.

Performance (that is, time to perform an operation) and the availability of the status information and access to the control functions of the Support Element is very dependent on the reliability, availability, and responsiveness of the customer network that interconnects the remote Hardware Management Console with the managed object. A remote Hardware Management Console monitors the connection to each Support Element and attempts to recover any lost connections and can report those connections that cannot be recovered.

Security for a remote Hardware Management Console is provided by the Hardware Management Console user logon procedures in the same way as a local Hardware Management Console. As with a local Hardware Management Console, all communication between a remote Hardware Management Console

and each Support Element is encrypted. Certificates for secure communications are provided, and can be changed by the user if wanted (see “Certificate Management” on page 84).

Note: When using Internet Explorer or Firefox 3.x browsers to access the Hardware Management Console or Support Element the Windows operating systems (Windows Vista and Windows 7) have changed how certificates are presented and authenticated to the operating system. If the domain name that you specify on the address bar is not listed in the certificate being presented to the client, the browser will let you know that the certificate cannot be authenticated to a trusted source. You can contact your IBM Service Support System for detailed instructions on resolving this issue.

TCP/IP access to the remote Hardware Management Console is controlled through its internally managed firewall and is limited to Hardware Management Console related functions. Hardware Management Console domain security (see “Domain Security” on page 103) may be used to isolate systems on a common LAN or to provide additional security. Individual remote users can be configured to have restricted access in the same way as they may be configured on a local Hardware Management Console.

Using a web browser

If you need occasional monitoring and control of managed objects connected to a single local Hardware Management Console, then the web browser is a good choice. An example of using the web browser might be an off-hours monitor from home by an operator or system programmer.

Each Hardware Management Console contains a web server that can be configured to allow remote access for a specified set of users. If a customer firewall exists between the web browser and the local Hardware Management Console, Table 5 shows the ports a web browser needs for communication to a Hardware Management Console.

Table 5. Ports used by a web browser for communications to the Hardware Management Console

Port	Use
tcp 443	Secure browser to web server communication
tcp 9960	Browser applet communication
tcp 9950-9959	Proxy support for Single Object Operation

After a Hardware Management Console has been configured to allow web browser access (see “Customize Console Services” on page 93 and “User Profiles” on page 124), a web browser gives an enabled user access to all the configured functions of a local Hardware Management Console, except those functions that require physical access to the Hardware Management Console such as those that use the local diskette or DVD media. The user interface presented to the remote web browser user is the same as that of the local Hardware Management Console and is subject to the same constraints as the local Hardware Management Console.

The web browser can be connected to the local Hardware Management Console using either a LAN TCP/IP connection or a switched (dial) network Point-to-Point Protocol (PPP) TCP/IP connection. Both types of connections can only use encrypted (HTTPS) protocols. If a switched connection is to be used, the PPP login name and password must be configured in the local Hardware Management Console (see “Customize Auto Answer Settings” on page 90) as well as the remote browser system. Logon security for a web browser is provided by the Hardware Management Console user logon procedures. Certificates for secure communications are provided, and can be changed by the user if wanted (see “Certificate Management” on page 84).

Performance (that is, time to perform an operation) and the availability of the status information and access to the control functions of the managed objects is very dependent on the reliability, availability, and responsiveness of the network that interconnects the web browser with the local Hardware

Management Console. Since there is no direct connection between the web browser and the individual managed objects, the web browser does not monitor the connection to each Support Element, does not do any recovery, and does not report any lost connections; these functions are handled by the local Hardware Management Console.

The web browser system does not require connectivity to IBM for service or support and maintenance of the browser and system level is the responsibility of the customer.

If the web address of the Hardware Management Console is specified using the format `https://xxx.xxx.xxx.xxx` (where `xxx.xxx.xxx.xxx` is the IPv4 address) or `https://[xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]` (where `xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx` is the IPv6 address) and Microsoft Internet Explorer is used as the browser, a host name mismatch message is displayed. To avoid this message, you can choose to do one of the following:

- Using the **Certificate Management** task on the Hardware Management Console, modify the **Subject Alternative Names** property from the Certificate Management window. In the **Modify DNS and IP Address** window, within the list of DNS entries, provide the IP address of the Hardware Management Console that you need in the web address of the Internet Explorer browser.

Note: The IP address of the Hardware Management Console is usually included in the list of IP Address entries for the Subject Alternative Names property and should not change.

- A Firefox browser should be used or a host name should be configured for the Hardware Management Console, using the **Customize Network Settings** task, and this host name should be specified in the web address instead of an IP address. Namely, using the format `https://hostname.domain_name` or `https://hostname` (for example, using `https://hmc1.ibm.com` or `https://hmc1`).

Web browser requirements

The Hardware Management Console web browser requires a supported web browser, a supported Java Virtual Machine (JVM), and cookie support in browsers that connects to it. Contact your support personnel to assist you in determining if your browser is configured with a supported Java Virtual Machine. It is required that the web browser uses the HTTP 1.1 protocol and if you are using a proxy server, the HTTP 1.1 protocol is enabled for the proxy connections.

Additionally, pop-ups must be enabled for all Hardware Management Consoles addressed in the browser if running with pop-ups disabled. For Firefox 4.0, Internet Explorer 8.0, and Internet Explorer 9.0 contact your support personnel for instructions on how to access the pop-ups and the security exception list.

The following browsers have been tested and include the recommended minimum Java SE Runtime Environment (JRE) update:

- Microsoft Internet Explorer 9.0 with JRE update 1.6.0_24.
- Microsoft Internet Explorer 8.0 or later with JRE update 1.6.0_24.

Note: Using this version can improve performance when accessing the Hardware Management Console remotely.

- Microsoft Internet Explorer 7.0 or later with JRE update 1.6.0_24 or later if you are using IPv6 addresses.

Note: If this browser is configured to use an internet proxy, then local intranet addresses should be included in the exception list, consult your network administrator for more information. If you still need to use the proxy to get to the Hardware Management Console, enable **Use HTTP 1.1 through proxy connections** under the **Advanced** tab in your Internet Options window.

- Firefox 4.0 with JRE update 1.6.0_24.
- Firefox 3.5.6 or later with JRE update 1.6.0_24.

Note: To make sure the JavaScript option to raise or lower windows and move or resize existing windows is enabled, go to **Tools** on the browser menu bar, select **Options...** from the list, select **Content** from the Options window, click **Advanced** that is displayed to the right of the **Enable JavaScript** option, select **Move or resize existing windows** and **Raise or lower windows** from the Advanced JavaScript Settings window, then click **OK** to enable.

Getting ready to use the web browser

Before you can use a web browser to access a Hardware Management Console, you must:

- Configure the Hardware Management Console to allow remote control for specified users.
- For LAN-based connections, know the TCP/IP address of the Hardware Management Console to be controlled, and have properly setup any firewall access between the Hardware Management Console and the web browser.
- For switched (dialed) connections, have configured the Hardware Management Console to accept incoming calls and know the PPP login name and password.
- Have a valid user ID and password assigned by the Access Administrator for Hardware Management Console web access.
- If you are using PPP, the Hardware Management Console must not already be configured as part of a 192.168.33.0/24 subnet to prevent routing problems when remote operation is being used.

Configuring the Hardware Management Console for web browser access from LAN or telephone connections

1. Log on to the Hardware Management Console with the ACSADMIN default user ID.
2. Open the **User Profiles** task. The User Profiles window is displayed.
3. For each user that you want to allow web browser access, select the user ID, point to **User** on the menu bar and when its menu is displayed, click **Modify**. The Modify User window is displayed.
4. Click **User Properties...** on the Modify User window, the User Properties window is displayed.
5. Select **Allow remote access via the web**, then click **OK**.
6. Open the **Customize Console Services** task. The Customize Console Services window is displayed.
7. Select **Enabled** on the **Remote operation** selection, click **OK**.

Logging on the Hardware Management Console from a LAN connected web browser

Use the following steps to log in to the Hardware Management Console from a LAN connected web browser:

1. Ensure that your web browser PC has LAN connectivity to the wanted Hardware Management Console.
2. From your web browser, enter the web address of the wanted Hardware Management Console, using the format `https://hostname.domain_name` (for example: `https://hmc1.ibm.com`), IPv4 address `https://xxx.xxx.xxx.xxx`, or IPv6 address `https://[xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]`.

If this is the first access of the Hardware Management Console for the current web browser session you can receive a certificate error. This certificate error is displayed if:

- The web server contained in the Hardware Management Console is configured to use a self-signed certificate and the browser has not been configured to trust the Hardware Management Console as an issuer of certificates, or
- The Hardware Management Console is configured to use a certificate signed by a Certificate Authority (CA) and the browser has not been configured to trust this CA.

In either case, if you know that the certificate being displayed to the browser is the one used by the Hardware Management Console, you can continue and all communications to the Hardware Management Console are encrypted.

If you do not want to receive notification of the certificate error for the first access of any browser session, you can configure the browser to trust the Hardware Management Console or the CA. In general, to configure the browser:

- You must indicate that the browser will permanently trust the issuer of the certificate, or
- By viewing the certificate and installing, to the database of trusted CAs, the certificate of the CA that issued the certificate used by the Hardware Management Console.

If the certificate is self-signed, the Hardware Management Console itself is considered the CA that issued the certificate.

3. When prompted, enter the user name and password assigned by your Access Administrator.

Configuring the Hardware Management Console for web browser access by telephone connections

Figure 56 displays the asynchronous PCS connections by modems.

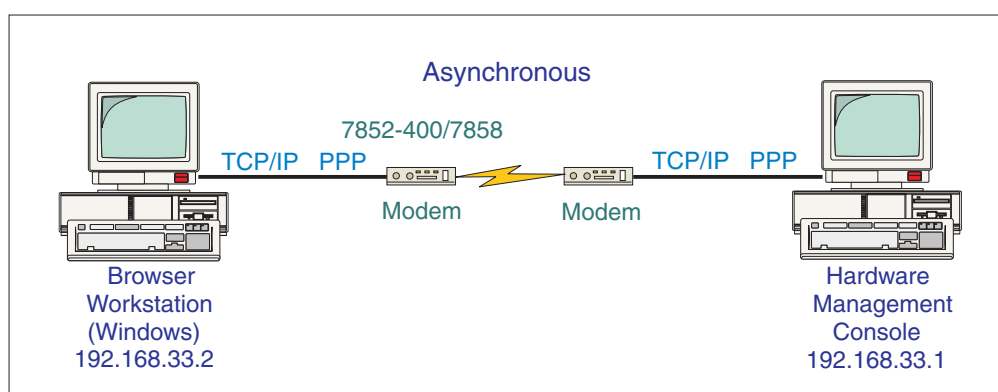


Figure 56. Asynchronous PCS connections via modems

Note: Call-home sessions may be deferred while phone line or modem are in use.

To use this facility, the Hardware Management Console must be configured to perform remote support facility functions using the asynchronous, TCP/IP connections.

1. Log on to the Hardware Management Console with Access Administrator access.
2. Open the **Customize Auto Answer Settings** task. The Customize Auto Answer Settings window is displayed.
3. Verify **Enable automatic call answering** is selected (a check mark is displayed).
4. Specify a **Modem telephone number**. This is the telephone number that must be dialed in order to reach the Hardware Management Console's modem.
5. Specify a **Login name**. This is the login name that must be used from the connecting browser system. It does not have to match any Hardware Management Console default user ID names. (Letters and numbers only, no spaces. This name is case sensitive and must be four to eight characters in length).
6. Specify a **Password**. This is the password that must be used from the connecting browser. It does not have to match any Hardware Management Console passwords. (Letters and numbers only, no spaces. This password is case sensitive and must be four to eight characters in length.)
7. Respecify your password in the **Confirm password** field, then click **OK**.
8. Log off the Hardware Management Console.

Using Windows XP to dial to a Hardware Management Console

1. Click **Start** and point to **Control Panel**. (Or you might have to point to **Settings** then **Control Panel**, depending how you are set up.) The Control Panel window is displayed.
2. Click **Network Connections** icon, the Network Connections window is displayed.

3. On the left side of the window, select **Create a new connection** under **Network Tasks**. The New Connection wizard window is displayed, click **Next** to continue.
4. Select **Connect to the network at my workplace**, click **Next** to continue.
5. Select **Dial-up connection**, click **Next** to continue.
6. Specify a *descriptive name* for the Hardware Management Console that is the target for this connection (for example, PRODUCTIONHMC) in the **Company Name** field, click **Next** to continue.
7. Specify the *telephone number* used to dial the Hardware Management Console in the **Phone number** field, click **Next** to continue.
8. Specify the **User name** and **Password** that you used in the **Customize Auto Answer Settings** task.
9. The Completing the New Connection Wizard window is displayed and the name of the connection you just created is displayed.
10. Click **Finish** to save this connection definition. The Connect xxxx window is displayed (where xxxx is the name you defined for the connection).
11. Click **Properties**. The xxxx Properties window is displayed (where xxxx is the descriptive name you defined for your connection).
12. Select the **Networking** tab.
13. Ensure that only the **Type of dial-up server I am calling** is **PPP**.
14. Ensure that the only protocol checked in **This connection uses the following items** is **Internet Protocol (TCP/IP)**, click **OK**.
15. The Connect xxxx window is displayed, click **Dial** to initiate the connection.

Logging on the Hardware Management Console using a defined dial connection entry

1. Click **Start**, point to **Settings**, then to **Network Connections**, and then to the descriptive name of the Hardware Management Console you want to connect with. The Connect with xxxx window is displayed.
2. Specify a **User Name** and **password** that exactly matches the **Login Name** and **password** that was specified in the **Customize Auto Answer Settings** dialog on the Hardware Management Console.
3. Click **Dial** to establish a dial connection.
4. Start your web browser (for example, Internet Explorer) using your normal procedures.
5. Enter https://192.168.33.1 as the target web address and press **Enter**.

Appendix D. Remote support facility

The Hardware Management Console Remote Support Facility (RSF) provides communication to a centralized IBM support network for hardware problem reporting and service. The types of communication provided include:

- Problem reporting and repair data
- Fix delivery to the service processor and Hardware Management Console
- Hardware inventory data
- On Demand enablement (optional).

The following security characteristics are in effect regardless of the connectivity method chosen:

- Remote Support Facility requests are always initiated from the Hardware Management Console to IBM. An inbound connection is never initiated from the IBM Service Support System.
- All data transferred between the Hardware Management Console and the IBM Service Support System are encrypted in a high-grade Secure Sockets Layer (SSL) encryption.
- When initializing the SSL encrypted connection the Hardware Management Console validates the trusted host by its digital signature issued for the IBM Service Support System.
- Data sent to the IBM Service Support System consists solely of hardware problems and configuration data. No application or customer data is transmitted to IBM.

Choose a connectivity method for remote support

You can configure the Hardware Management Console to send hardware service-related information to IBM by using a dialup connection over a modem or using an Internet-based connection. The advantages to using an Internet connection include:

- Faster transmission speed
- Ability to send more data on an initial problem request potentially resulting in more rapid problem resolution
- Reduced customer expense (for example, the cost of a dedicated analog telephone line)
- Greater reliability.

Unless your enterprise's security policy prohibits any connectivity from the Hardware Management Console over the Internet, an Internet connection is recommended.

Note: You can choose to configure a Hardware Management Console for both Internet and modem connectivity. In this case, the Hardware Management Console tries to establish an Internet connection first and treats modem connectivity as a backup mechanism, if the Internet connection is not successful.

Modem connectivity

Figure 57 on page 224 displays a typical dial environment. This configuration allows the Hardware Management Console to use a modem into the AT&T global network, through which connections are made to the IBM Service Support System. The Hardware Management Console automatically detects the modem when it initializes.

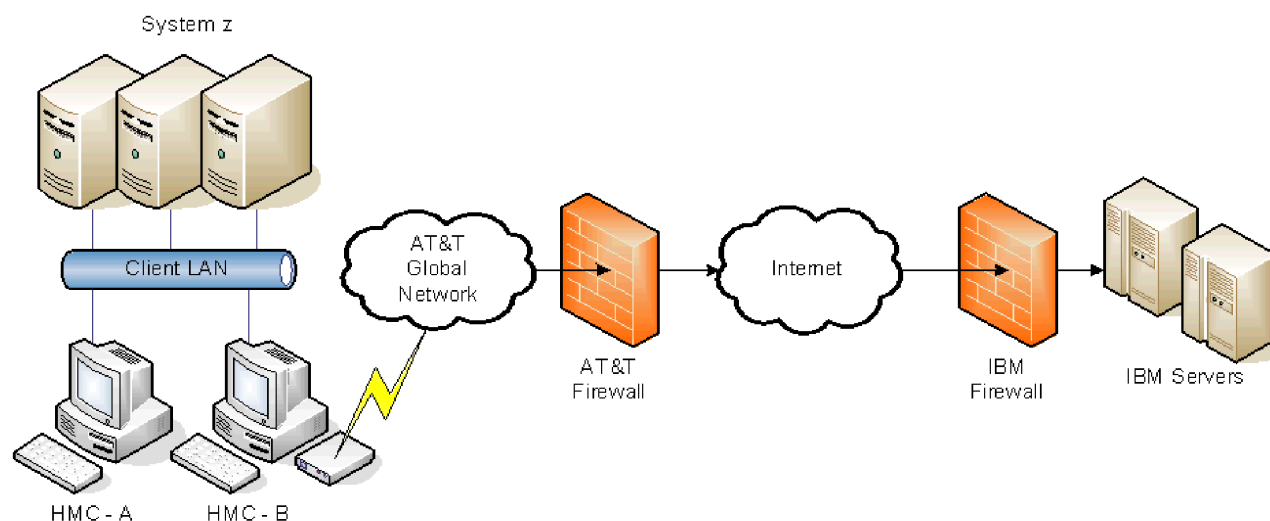


Figure 57. Modem connectivity

If a modem is used, you must provide a dedicated analog line to connect to the modem of the Hardware Management Console. The Hardware Management Console uses one of the configured telephone numbers to dial the modem, and connects to the Global Network. The Hardware Management Console creates a TCP/IP connection through a *fenced internet*, which completes the network between the Hardware Management Console and the IBM servers.

The *fenced internet* connection uses a firewall to limit access between the Hardware Management Console and the Internet. Specifically, it allows communication only between the Hardware Management Console and a list of IBM IP addresses. All other access to and from the Internet is blocked.

Note: Phone (data) line quality may impact modem performance resulting in transmission or connection delays (up to two minutes) as the modem attempts to negotiate a reliable data transmission speed.

Internet connectivity

The Hardware Management Console can be configured to use an existing Internet connection to connect to the IBM Service Support System. All the communications are handled through TCP sockets initiated by the Hardware Management Console and use a high-grade SSL to encrypt the data that is transmitted. The destination TCP/IP addresses are published to enable you to set up firewalls allowing connection.

Note: The standard HTTPS port 443 is used for all communications.

When an internet connection is used, the Hardware Management Console can be configured to use a second network card to physically separate a private LAN connection from the Internet-enabled network. Also, depending upon your network configuration, the Hardware Management Console may be able to connect to IBM service and support using the IPv4 (basic) and/or IPv6 internet. From the **Customize Outbound Connectivity** task use the **Protocol to Internet** selection on the **Internet** tab to choose the appropriate setting.

The Hardware Management Console can be enabled to connect directly to the Internet (see Figure 58 on page 225) or to connect indirectly from a customer-provided proxy server (see Figure 59 on page 225). The decision about which of these approaches works best for your installation depends on the security and networking requirements of your enterprise.

Hardware Management Console direct internet SSL connection

If your Hardware Management Console can be connected to the Internet, and the external firewall can be set up to allow established TCP packets to flow outbound to the destinations described in “IBM server address list” on page 226, you can use a direct Internet connection (see Figure 58 for a sample configuration). The use of Source Network Address Translation (SNAT) and masquerading rules to mask the Hardware Management Console's source IP address are both acceptable.

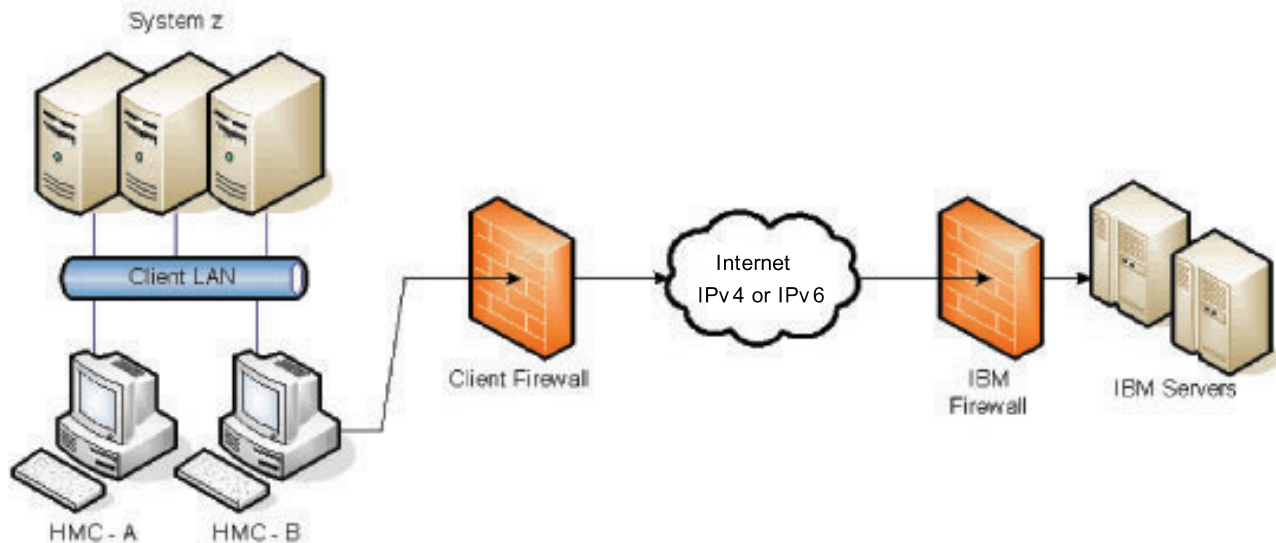


Figure 58. SSL connectivity

Using an indirect internet connection with proxy server

If your installation requires the Hardware Management Console to be on a private network, you may be able to use internet connect indirectly using an SSL proxy, which can forward requests to the internet (see Figure 59 for a sample configuration). One of the other potential advantages of using an SSL proxy, is that the proxy may support logging and audit facilities.

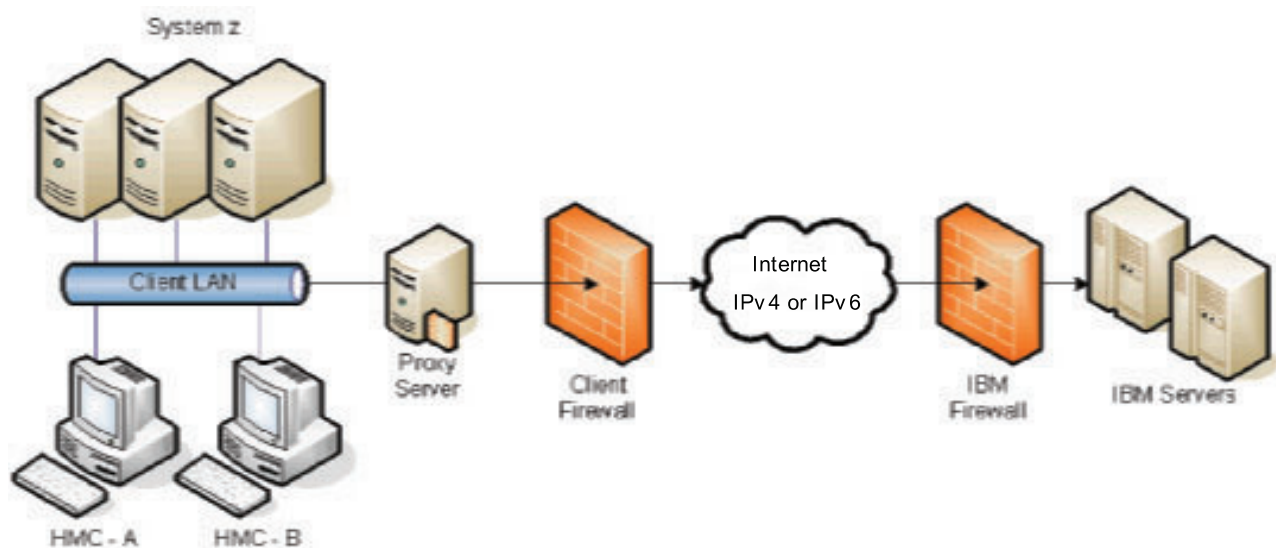


Figure 59. SSL with proxy server connectivity

To forward SSL sockets, the proxy server must support the basic proxy header functions (as described in **RFC 2616**) and the **CONNECT** method. Optionally, basic proxy authentication (**RFC 2617**) may be configured so that the Hardware Management Console authenticates before attempting to forward sockets through the proxy server.

For the Hardware Management Console to communicate successfully, the client's proxy server must allow connections to port 443. You can configure your proxy server to limit the specific IP addresses to which the Hardware Management Console can connect. See “IBM server address list” for a list of IP addresses.

Depending upon your configuration, the Hardware Management Console may be able to connect to your SSL proxy using a different Internet Protocol than what is required for the proxy to connect to the internet. In this case, the value selected in **Protocol to Internet** on the **Internet** page from the **Customize Outbound Connectivity** task must reflect the Internet Protocol used by the SSL proxy to connect to the internet. For example, the Hardware Management Console may connect to your SSL proxy using an IPv6 address, but the proxy may be configured to connect to the internet using IPv4. In this case, you would enter the IPv6 address of your SSL proxy server on the **Internet** page, but select IPv4 for **Protocol to Internet** from the **Customize Outbound Connectivity** task.

IBM server address list: The Hardware Management Console uses the following IP addresses (depending on your Hardware Management Console version) when it is configured to use Internet connectivity. All connections to these IP addresses use port 443 TCP. The IP addresses you must allow depends on the protocol you are using.

- For Hardware Management Consoles at Version 2.10.0 or earlier, you must allow access to the following IPv4 addresses:
 - 129.42.160.48 and 207.25.252.200 (allow Hardware Management Console access to System Authentication Server (SAS))
 - 129.42.160.49 and 207.25.252.204 (allow Hardware Management Console access to IBM Service for North or South America)
 - 129.42.160.50 and 207.25.252.205 (allow Hardware Management Console access to IBM Service for all other regions)

Note: You only need to specify the IP address necessary to set up access to SAS and those appropriate for your region.

- For Hardware Management Consoles at Version 2.10.0 or later, internet connectivity to the IBM Service Support System has been enhanced to enable access from the IPv6 internet as well as the IPv4 internet. If you require access to the IBM Service Support System using the IPv6 internet, you must allow access to all of these additional addresses:
 - 2620:0:6C0:1::1000
 - 2620:0:6C1:1::1000
 - 2620:0:6C2:1::1000
- For Hardware Management Consoles at Version 2.10.1, Internet Protocol addresses using IPv4 requires outbound connectivity to the following IP addresses:
 - 129.42.26.224
 - 129.42.34.224
 - 129.42.42.224

Using multiple call-home servers

To avoid a single point of failure, it is recommended that each Support Element and Hardware Management Console be configured to use multiple call-home servers. The first available call-home server attempts to handle each service event. If the connection or transmission fails with this call-home server the service request is tried again using the other available call-home servers until one is successful or all have been tried.

A Support Element can call-home service events using any Hardware Management Console (at its release level or higher) that has been configured for outbound connectivity and has been configured as a call-home server when the CPC object was defined to the Hardware Management Console.

A Hardware Management Console can call-home service events Using any Hardware Management Console that has been automatically discovered or has been manually configured using the **Customize Outbound Connectivity** task. A Hardware Management Console is discovered under the following circumstances:

- It is at the same level or higher as the source Hardware Management Console.
- It has been enabled to call-home and the Outbound Connectivity Settings window has been configured.
- It is configured to communicate on the same TCP/IP subnet as the source Hardware Management Console.

Appendix E. Using the System (Sysplex) Time task

Use this task to view or setup time synchronization for a server (CPC) using the Sysplex Timer and/or the Server Time Protocol (STP).

A *Sysplex Timer* is a device that provides a time source to the time-of-day (TOD) clocks of Central Processor Complexes (CPCs) attached to it and the operating systems or control programs running on that server (CPC). A feature called an External Timer Reference (ETR) installed in the server (CPC) provides two ETR attachment facility (EAF) ports for attaching Sysplex Timers. Both ports may attach the same Sysplex Timer, or each port may attach a separate Sysplex Timer when configured with 9037 Expanded Availability.

An ETR network consists of one Sysplex Timer or coupled Sysplex Timers (Expanded Availability), and the links from this source to the systems. Each system has two ETR Attachment Facility (EAF) ports which can be connected by a link to the Sysplex Timer.

Note: An ETR network is available only on System z9 and System z10 servers (CPCs).

Server Time Protocol (STP) is a time synchronization architecture designed to provide the capability for multiple servers (CPCs) to maintain time synchronization with each other and to form a Coordinated Timing Network (CTN). STP is designed for servers (CPCs) that have been configured to be in a Parallel Sysplex® or a sysplex (without a Coupling Facility), as well as servers (CPCs) that are not in a sysplex, but need to be time synchronized. STP is designed as a message-based protocol allowing timekeeping information to be sent between servers (CPCs) and Coupling Facilities (CFs) over InterSystem Channel-3 (ISC-3) links configured in peer mode, Integrated Cluster Bus-3 (ICB-3) links (System z9 only), Integrated Cluster Bus-4 (ICB-4) links (System z9 or System z10 only), or InfiniBand (IFB) links.

There are two types of CTNs supported by STP: Mixed and STP-only. A *Mixed CTN* is a timing network that contains a collection of servers (CPCs), and has at least one STP-configured server (CPC) stepping to timing signals provided by the Sysplex Timer. The CTN ID must have a valid STP network ID and the ETR network ID must be in the range of 0 to 31. The *STP-only CTN* is a timing network that contains a collection of servers (CPCs) configured to be in STP timing mode. None of the servers (CPCs) in an STP-only CTN can be in ETR timing mode.

The feature or features you have installed on the server (CPC) determines the tasks that are available in the System (Sysplex) Time window:

- If only the ETR feature is installed, the System (Sysplex) Time window displays the current configuration and the status of the ETR Attachment Facility (EAF) ports that allow you to synchronize to the Sysplex Timers for your server (CPC). The following tabs appear in the System (Sysplex) Time window:
 - ETR Configuration
 - ETR Status
- If the ETR feature is installed and the Server Time Protocol (STP) feature is enabled, the System (Sysplex) Time window displays the following tabs:
 - Timing Network
 - Network Configuration
 - ETR Configuration
 - ETR Status
 - STP Configuration
 - STP Status
 - ETS Configuration

- If only the Server Time Protocol (STP) feature is enabled the System (Sysplex) Time window displays the following tabs:
 - Timing Network
 - Network Configuration
 - STP Configuration
 - STP Status
 - ETS Configuration

The following sections of this Appendix provides a brief description of each of the tabs that are displayed from the System (Sysplex) Time window as shown in Figure 60. There is also a list of STP terms to help you better understand the **System (Sysplex) Time** task, see “STP terminology” on page 236.

Use the online Help if you need additional information about the **System (Sysplex) Time** task. You can also go to Resource Link, <http://www.ibm.com/servers/resourcelink>, click **Education** in the navigation bar, choose the appropriate **Mainframe**, then select **Introduction to Server Time Protocol (STP)**.

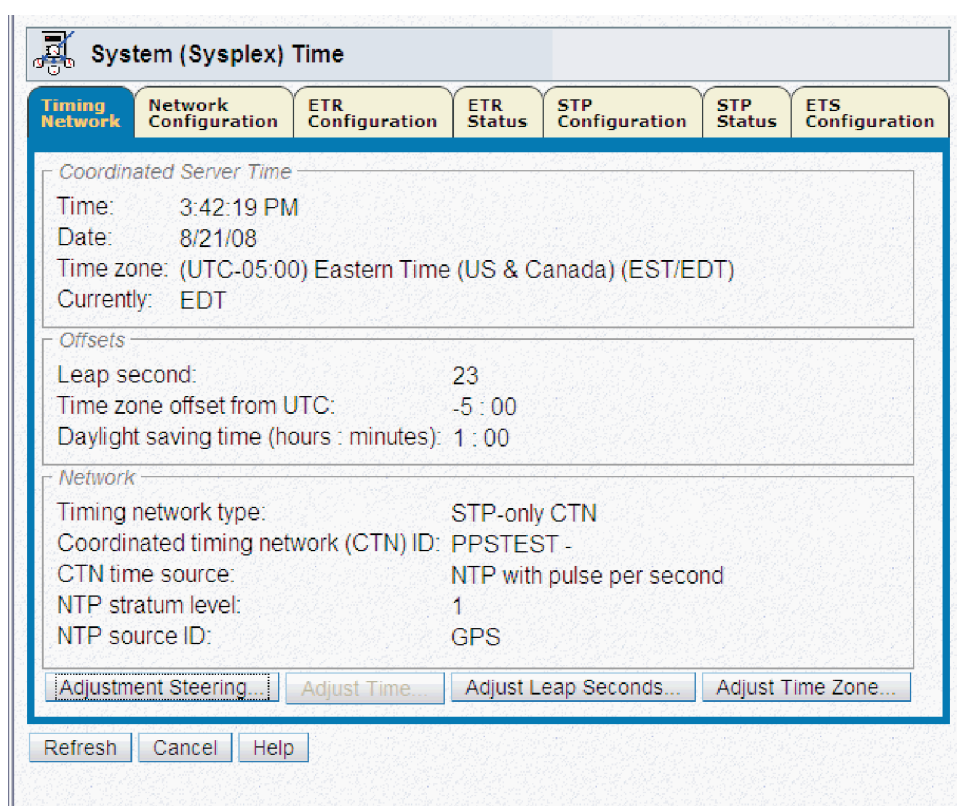


Figure 60. System (Sysplex) Time window

Timing network

You can use this tab to view the settings of the timing network. This window displays overall timing information for the ETR network or Coordinated Timing Network (CTN) including the current date and time, local time offsets, and general timing network information. The information displayed in this window is identical on each server in the same ETR network or CTN.

In an STP-only CTN adjustments can be made for the management of time, leap seconds, and time zones. These adjustments are available on every server in the STP-only CTN but are only enabled on the Current Time Server to ensure that all time and offset adjustments are done at the server providing time

information to all members of the STP-only CTN. Any changes that are made are sent to the Current Time Server (CPC) or the server (CPC) being set up to be the Current[®] Time Server. From there they are distributed throughout the timing network.

- Click **Adjustment Steering...** to view the detailed steering information for the entire STP-only CTN. The Adjustment Steering Information window is displayed. It indicates the status of the adjustment and the amount of time the clock is currently being adjusted by or was last adjusted by. Each server (CPC) is gradually adjusting its clock by steering towards the new Coordinated Server Time (CST).
Adjustment steering could be the result of the following:
 - Setting the time manually on the console
 - Dialing out to the external time source using the Hardware Management Console
 - Migrating from an STP-only CTN to a Mixed CTN
 - Accessing an External Time Source (ETS) via Network Time Protocol (NTP) or NTP with pulse per second (PPS).
- Click **Adjust Time...** to make an adjustment to the current CST. The Adjust Time window is displayed. Click **Access External Time Source** to get the adjustment amount from an external time source (if one is set up) or manually enter an amount, then click **OK** to send the amount specified to the STP facility.

Note: This action is not available when the time source for the Coordinated Timing Network (CTN) is **NTP with pulse per second (PPS)**.

- Click **Adjust Leap Seconds...** to change the leap seconds. The Adjust Leap Seconds Offset window is displayed. Specify a new leap second offset and when that adjustment should happen, click **OK** to have the new leap second amount or changed schedule time take affect.
- Click **Adjust Time Zone...** to change the time zone or daylight saving time. The Adjust Time Zone Offset window is displayed. Click **Define...** to access the Define Time Zone Algorithm window to allow you to set up a time zone not found in the list of time zones. Make further changes to the daylight saving time start and end, then click **OK** to save your changes.

Network configuration

You can use this tab to view the current STP-only CTN configuration and any configuration in progress including migration from an STP-only CTN to a Mixed CTN. Changes made in this window affect all servers (CPCs) that are members of the STP-only CTN. The changes are sent to the Current Time Server (CPC) or the server (CPC) being set up to be the Current Time Server. From there they are distributed throughout the timing network. The information displayed in this window is the same for all servers (CPCs) participating in the same CTN.

- Click **Apply** when you are ready to send a new configuration for the STP-only CTN to the STP facility or to migrate from an STP-only CTN to a Mixed CTN. **Apply** is disabled until the initial values are set in the STP-only CTN.

Note: When the time source for the CTN is NTP with pulse per second, you are not allowed to migrate from an STP-only CTN to a Mixed CTN until you stop using PPS as the ETS.

- Click **Initialize Time...** to set up initial time values for a server (CPC) that will act as the Current Time Server for a CTN. The Initialize Time window is displayed where you can set leap second offset, time zone, or date and time, click **OK** to proceed.
- Click **Deconfigure** to unconfigure the Preferred Time Server (CPC), Backup Time Server (CPC), and Arbiter.

Note: This action is disruptive.

Consider this action only if you no longer want the STP-only CTN configured with a Preferred Time Server (CPC), Backup Time Server (CPC), and Arbiter, where the Current Time Server is providing time information to your entire STP-only CTN.

- Click **Cancel Migration to Mixed CTN** if you decide not to proceed with the migration of an STP-only CTN to a Mixed CTN.

ETR configuration

Note: This tab is not available for zEnterprise System servers (CPCs).

You can use this tab to perform the following activities, then click **Apply** to proceed:

- Set the configuration for the ETR Attachment Facility (EAF) ports to synchronize your server (CPC) to your Sysplex Timer.
- Configure your server (CPC) to participate in a Mixed CTN by specifying an ETR network ID.
- Migrate your server (CPC) from a Mixed CTN to an STP-only CTN by removing the ETR network ID.
- Remove the ETR network ID to no longer be part of an ETR network or Mixed CTN.

This tab is displayed only when an ETR feature is installed in the server (CPC). Configuration changes made on this window affect only this particular server (CPC). They are not applied to an entire timing network.

ETR status

Note: This tab is not available for zEnterprise System servers (CPCs).

You can use this tab to view the configuration and operational state of the ETR connections as viewed by the server (CPC). Modifications that are made from the Sysplex Timer console, such as setting the ETR network and ETR Unit IDs, are displayed on this page. The **ETR Status** tab is displayed only when an ETR feature is installed in the server (CPC).

STP configuration

You can use this tab to:

- Configure this server (CPC) or remove it from participating in a Mixed CTN.
- Configure this server (CPC) or remove it from participating in an STP-only CTN.

Configuration changes made on this window only affect this particular server (CPC). They are not applied to an entire timing network.

Note: When a server (CPC) does not have the ETR feature installed, a decimal number from 0 to 31 can be specified in the ETR network ID portion of the CTN ID so that the server (CPC) can participate in a Mixed CTN.

STP status

Use this tab to view the STP status information for a specific server (CPC) as shown in Figure 61 on page 233. The information that you are viewing includes:

- **Timing state** - indicates the timing state the server (CPC) is operating in. If it has a value of anything other than *Synchronized* then the server is not actively participating in an ETR network or CTN.
- **Usable clock source** - indicates whether a usable clock source is available in order to synchronize the server TOD.
- **Timing mode** - indicates the timing mode of the server within the ETR network or CTN.
- **Stratum level** - indicates the hierarchy of this server within the timing network. A stratum level of 0 indicates the server has no time source.

- **Maximum timing stratum level** - contains a number indicating how far a server can be from the Stratum 1 and still be in a synchronized state. The stratum level indicates the hierarchy of this server within the timing network. A stratum level of 0 indicates the server has no time source, and a stratum level of n indicates the server is $n-1$ hops away from the Stratum 1.
- **Maximum STP version** - contains the maximum STP facility level supported by this server (CPC).
- **System Information** - this table identifies the remote servers which are directly attached to this server for STP purposes.
- **Local Uninitialized STP links** - this table identifies this server's (CPC's) coupling links that may be used to exchange STP messages with other servers.

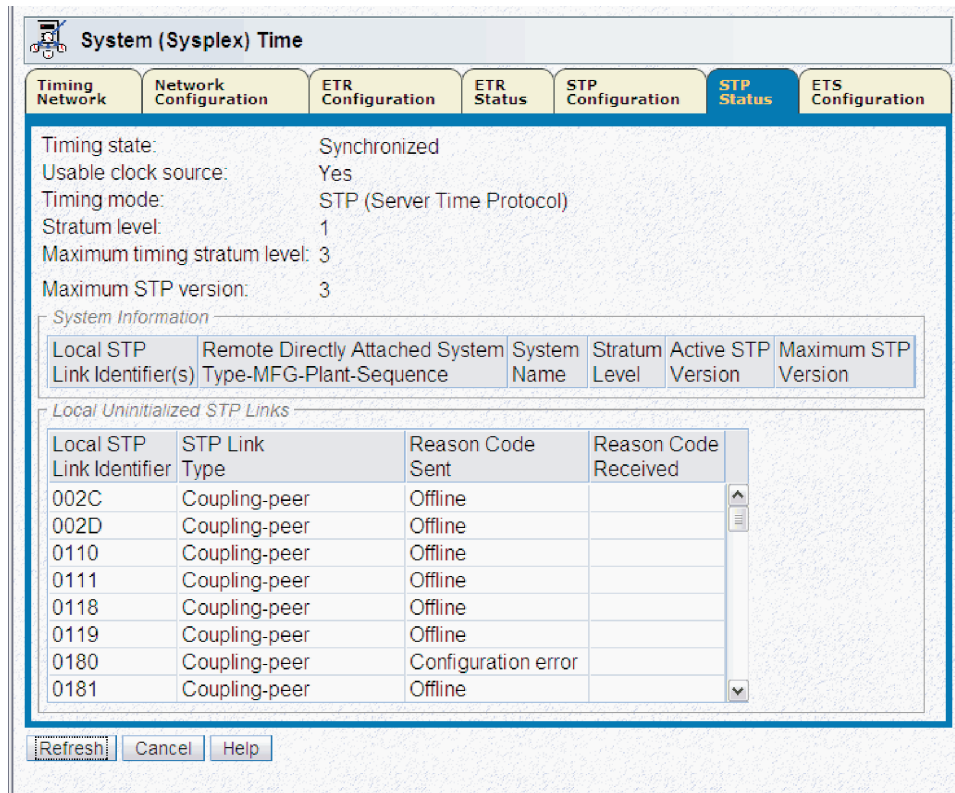


Figure 61. STP status page

ETS configuration

You can use this tab to view or modify the External Time Source (ETS) configuration information for a specific server (CPC). This tab is available only when Network Time Protocol (NTP) support is available.

Using this page depends on the role of the CPC in the STP-only CTN. The note that is displayed on the top of the page indicates the role of the CPC and recommends the actions that should be taken.

If the server (CPC) does not require an External Time Source (ETS) to be configured or if it will be dialing out to the ETS using the Hardware Management Console, select **Use dial out if configured on Hardware Management Console** (the default setting).

Note: If the ETS is accessed via dial out, it is set by using the **Customize Outbound Connectivity** task on the Hardware Management Console, then selecting the **External Time Source** tab from the Customize

Outbound Connectivity window. The **External Time Source** page is used to set up the modem parameters to be used when dialing an ETS in support of servers (CPCs) that are participating in an STP-only CTN.

The **Customize Outbound Connectivity** task is *not* required if your ETS is provided by a Network Time Protocol (NTP) server.

If the server (CPC) requires access to an NTP server as the ETS, select **Use NTP**. In this case, the **NTP Time Server Information** is displayed on the **ETS Configuration** page, as shown in Figure 62. It allows up to two NTP servers to be configured for use and displays information about these servers. In addition, it allows the ability to test access to other NTP servers without modifying the current configuration.

System (Sysplex) Time

Timing Network | Network Configuration | ETR Configuration | ETR Status | STP Configuration | STP Status | **ETS Configuration**

Note
This CPC has the role of Current Time Server for an STP-only CTN. If you plan to attach to an ETS device, an ETS configuration is required. Changes made to the ETS configuration have an immediate effect on the time source for the CTN.

External Time Source (ETS)
☐ Use dial out if configured on Hardware Management Console
☒ Use NTP
☐ Use NTP with pulse per second (PPS)

NTP Time Server Information

Select	Configured	NTP Time Server	Stratum	Source	Status
☒	☒	9.56.192.87	1	GPS	Success
☐	☐	9.56.192.88			

Apply Query

Refresh Cancel Help

Figure 62. ETS configuration page using the NTP option

If the server (CPC) requires access to an NTP server with enhanced time accuracy, select **Use NTP with pulse per second (PPS)** as shown in Figure 63 on page 235. This option adds the capability to configure an NTP server that has a PPS output signal as the ETS device. In this case, the *NTP Time Server Information* section is displayed on the **ETS Configuration** page with one additional column, **PPS Port**, used to coordinate the NTP server with the appropriate PPS port on the zEnterprise System, System z10 or System z9 server. A configured NTP server has to be connected to the Support Element LAN, and the PPS output of the same NTP server has to be connected to the PPS input provided on the External Time Reference (ETR) card of the System z10 or System z9 server or the FSP/STP card of the zEnterprise System.

A section for PPS port status is also displayed in the *NTP Time Server Information* section, showing the status of each PPS port. An STP-only CTN, configured to use NTP with pulse per second (PPS) as the ETS, can keep CST synchronized to within 10 microseconds of the ETS.

Use the online Help for additional information.

System (Sysplex) Time

Timing Network | Network Configuration | **ETR Configuration** | ETR Status | STP Configuration | STP Status | **ETS Configuration**

Note
This CPC has the role of Current Time Server for an STP-only CTN. If you plan to attach to an ETS device, an ETS configuration is required. Changes made to the ETS configuration have an immediate effect on the time source for the CTN.

External Time Source (ETS)
☐ Use dial out if configured on Hardware Management Console
☐ Use NTP
☒ Use NTP with pulse per second (PPS)

NTP Time Server Information

Select	Configured	PPS Port	NTP Time Server	Stratum	Source	Status
☒	☒	0	9.56.192.87	1	GPS	Success
☐	☐	1	9.56.192.88			

PPS Port Status
 Port 0: Tracking to PPS signal
 Port 1: Not configured

Apply Query

Refresh Cancel Help

Figure 63. ETS configuration page using the NTP with PPS option

PPS control

Note: This tab is available only for zEnterprise System servers (CPCs).

You can use this tab to diagnose problems with a pulse per second (PPS) port. This page, as shown in Figure 64 on page 236, accomplishes the following:

- Displays whether PPS signals are detected at a PPS port
- Allows internal diagnostics to be run on each port
- Displays when a port has been fenced by Licensed Internal Code
- Allows a port to be reset.

Note: This tab is available only by a service representative or a user ID that is assigned service representative roles.

To setup and perform an internal diagnostic test on a PPS port:

1. Verify that the PPS port to be tested is not configured for PPS use. If it is configured, uncheck the Configured column for the appropriate PPS port (from the **ETS Configuration** tab), then click **Apply**.
2. Verify there is no active PPS cable connected to the PPS port to be tested.
3. Select the **PPS Control** tab to perform an internal diagnostic test on a PPS port.
4. Select **Test**, then click **Apply**.
5. Click **Internal Test**, after the button becomes enabled, to run an internal diagnostic test on the port to determine whether or not the PPS hardware is functioning properly.

- When finished with the test, select **PPS input**, then click **Apply** to allow the port to receive PPS signals from an ETS.

Use the online Help for additional information.

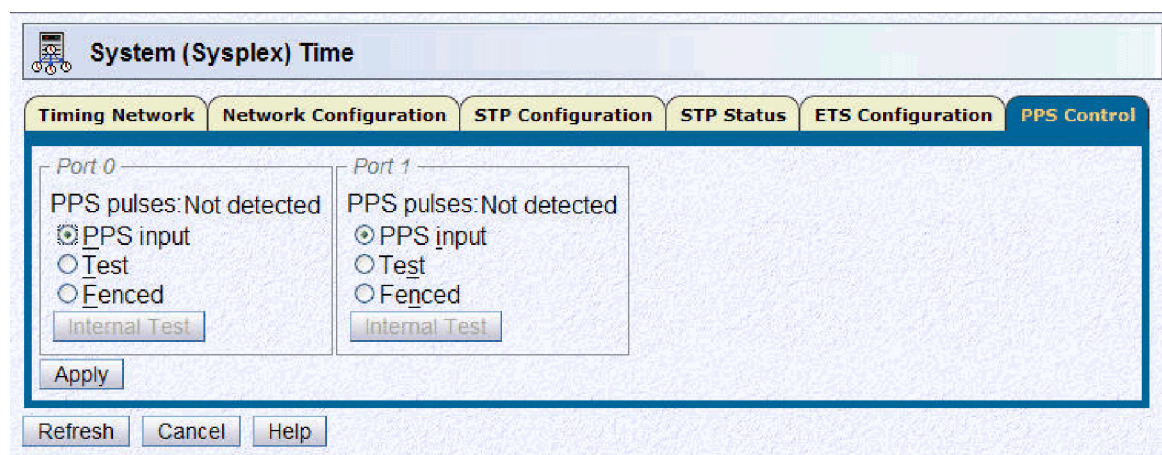


Figure 64. PPS control page

STP terminology

This section provides a summary of the STP terminology that is used in this Appendix and in the online help.

Arbiter

Server (CPC) assigned by you to provide additional means for the Backup Time Server to determine if it should take over as the Current Time Server.

Backup Time Server

Server (CPC) assigned by you to take over as the Current Timer Server (Stratum 1 Server), either because of a planned or unplanned reconfiguration.

Coordinated Server Time (CST)

The CST in a CTN represents the time for the CTN. CST is determined at each server (CPC) in the CTN.

Coordinated Timing Network (CTN)

Network that contains a collection of servers (CPCs) that are time synchronized to Coordinated Server Time (CST). All STP-configured servers (CPCs) in a CTN must have the same identifier, referred to as a CTN ID.

Coordinated Timing Network Identifier (CTN ID)

Identifier that is used to indicate whether the server (CPC) has been configured to be part of a CTN and, if so, identifies that CTN. This is made up of two fields: one that defines the STP network ID and one that defines the ETR network ID.

Current Time Server

Server (CPC) that is currently the Stratum 1 for an STP-only CTN.

ETR Network

Network that contains a collection of servers (CPCs) that are time synchronized to the Sysplex Timer. All servers (CPCs) in the ETR network must have the same ETR network ID.

ETR Network ID

Second field of CTN ID whose low order 5 bits define the ETR network that the server (CPC) is configured for. The ETR network ID is 0 to 31 if the server (CPC) is part of the ETR network otherwise it is not specified when an STP-only CTN is configured.

ETR Timing Mode

The TOD clock has been initialized to the Sysplex Timer and is being stepped by stepping signals from the Sysplex Timer.

External Time Source (ETS)

Provides the ability to accurately set the time to a standard time source instead of setting the time manually.

Local Timing Mode

The Time of Day (TOD) clock has been initialized to a local time and is being stepped at the rate of the local hardware oscillator.

Mixed Coordinated Timing Network (Mixed CTN)

Timing network that contains a collection of servers (CPCs), and has at least one STP-configured server (CPC) stepping to timing signals provided by the Sysplex Timer. STP-configured servers (CPCs) in the Mixed CTN not stepping to the Sysplex Timer achieve synchronization by exchanging STP messages. The CTN ID must be a valid STP network ID and the ETR network ID must be in the range of 0 to 31.

Network Time Protocol (NTP)

Used to synchronize the time of a computer client or server to another server or reference time source. Typical NTP configurations use multiple redundant servers and diverse network paths in order to achieve high accuracy and reliability.

PPS Pulse per second. An electrical signal that precisely indicates the start of a second. PPS signals are output by various precision clocks and are used for precise timekeeping and time management. Combining the PPS functionality with a reliable NTP time server allows for better date and time accuracy and preciseness.

Preferred Time Server

Server (CPC) assigned by you to be the Preferred Stratum 1 Server in an STP-only CTN.

STP Network ID

First field of the CTN ID that defines the STP network that the server (CPC) is configured for. When the STP-network ID is not specified, the server (CPC) is not configured to be part of a CTN.

STP-only Coordinated Timing Network (STP-only CTN)

Timing network that contains a collection of servers (CPCs) configured to be in STP timing mode. None of the servers (CPCs) in an STP-only CTN can be in ETR timing mode.

STP Timing Mode

The TOD clock has been initialized to CST and is being stepped at the rate of the local hardware oscillator, and is steered to maintain, or attain, synchronization with CST.

Stratum

A means to identify the hierarchy of the server (CPC) within the timing network.

Stratum 0 Level

A stratum level of zero is used to indicate that the stratum level is undefined.

Stratum 1 Server

Highest level in the hierarchy of a timing network that uses STP messages for synchronization. In a Mixed CTN any STP-configured server (CPC) synchronized to the Sysplex Timer is a Stratum 1 server (CPC), therefore multiple Stratum 1 servers (CPCs) can exist. In an STP-only CTN the Current Time Server is the Stratum 1 server (CPC).

Stratum 2 Server

Server that uses STP messages to synchronize to a Stratum 1 server (CPC).

Stratum 3 Server

Server that uses STP messages to synchronize to a Stratum 2 server (CPC).

Appendix F. Changing your time-of-day clock

Your operating system time is set and updated by the CPC Time-of-Day (TOD) clock. This clock is set either to your local time or to the Coordinated Universal Time (UTC).

The Hardware Management Console can set its own time zone using the **Customize Console Date/Time** task. However, the Hardware Management Console synchronizes its time with the Support Element that has been defined as a master time source (see “Add Object Definition” on page 181 and “Change Object Definition” on page 182 to **Enable for time synchronization**). When the Hardware Management Console does this, it converts the Support Element's time from the Support Element's time zone to its own time zone. It does not change its own time zone. For example, the Support Element is on the New York time zone and the Hardware Management Console is in Chicago, then when the Support Element is set to 9:00 am, the Hardware Management Console is set to 8:00 am.

The following procedures are used for changing your TOD clock depending on whether a time source (such as ETR or STP) has been enabled.

Note: You must specify a time zone (other than Local) for your Hardware Management Console and for the Support Elements at Version 2.9.0 or later.

Setting the Hardware Management Console date and time

The Hardware Management Console's time zone needs to be set even if the Hardware Management Console was set up to use the CPCs Support Element as a time source (see “Add Object Definition” on page 181 and “Change Object Definition” on page 182 to **Enable for time synchronization**). However, the Hardware Management Console's time cannot be set if a Support Element is acting as the time source. Use the following steps to set the Hardware Management Console TOD clock.

1. Open the **Customize Console Date/Time** task.
2. The Customize Console Date and Time window is displayed. Verify the time, date, and time zone. If it is correct, click **Cancel**. If a correction is needed, enter your changes and click **Customize**.

Note: You should not specify **Local** when the time zone specifies **not initialized**. That combination does not guarantee that the actual time zone that is being used is what you really want.

3. Click **OK**.
4. The Customize Console Date and Time window is displayed again. Click **Cancel** when this task is complete.

Setting the Support Element time zone

When the time zone is changed at the time source, each CPC is notified of the change and the operating system adjusts its time zone to that of the time source. Because there was no change to the Coordinated Universal Time (UTC), the Support Element(s) is not notified of a change.

To set or update the Support Element(s) clock's time zone, use the following steps:

1. Open the group that contains the object with the Support Element that you want to connect to.
2. Select one CPC.
3. Open the **Single Object Operations** task under **Recovery** tasks. The Single Object Operations Task Confirmation window is displayed.
4. If you want to continue establishing a session with a single CPC console, click **Yes**. The Primary Support Element window is displayed.

5. Open the **Customize Support Element Date/Time** task.
6. The Customize Support Element Date and Time window displays the current Support Element clock, date, time, and time zone. Enter the new information, then click **Use New Time....**
7. The Customize Support Element Date and Time Confirmation window is displayed, then click **Yes**.
8. The Customize Support Element Date/Time Progress window is displayed.
Then the message "System (Sysplex) time is in use. Your input will not be used to set the battery operated clock." displays in the status field.
This message means that the Support Element detected an active time source and updated its date, time, and time zone to match that of the time. Click **OK**.

Setting the Support Element time

This section describes the actions to take when setting the time depending on whether or not a time source (such as ETR or STP) is enabled.

Time source enabled

Attention: Issuing a set time on a Sysplex Timer (9037) may cause any running operating systems to enter a disabled wait state. Consult your operating system documentation for details.

If the ETR, which uses the Sysplex Timer (9037), is installed in the processor complex, the time, date, and offset from the Sysplex Timer will be used to set the time-of-day in all attached CPCs. If you need to correct the time, change the time at the ETR.

If Server Time Protocol (STP) is enabled in the CPC, the time, date, and offsets from the Current Time Server will be used to set the time-of-day. If you need to correct the time-of-day, adjust the time at the current server.

Time source not enabled

The Support Element(s) contain a battery operated TOD clock. The CPC TOD clock will be set using the Support Element TOD when the system is activated.

Use the following steps to correct the date or time in the Support Element(s):

1. Select a group of defined CPCs or an individual CPC.
2. Open the **Customize Support Element Date/Time** task under **Operational Customization** tasks.
3. The Customize Support Element Date and Time window displays the current Hardware Management Console clock, date, time, and time zone. Enter the new information, then click **Use New Time....**

Note: Depending on your machine type and model the Support Element **Clock** and **Time zone** fields cannot be modified by the Hardware Management Console. In that case, you must use the **Single Object Operations** task to set the Support Element clock and time zone.

4. The Customize Support Element Date and Time Confirmation window is displayed. Click **Yes**.
5. The Customize Support Element Date/Time Progress window is displayed. Click **OK** to continue with the task.

Attention: The following steps will disrupt the operating system if it is running, and should only be performed if the CPC TOD needs to be updated now.

Note: These steps assume that the activation profiles have been set up for each CPC.

Use the following steps to correct the CPC TOD:

1. Select a group of defined CPCs or an individual CPC.
2. Open the **Activate** task under **Daily** tasks.

Level 01a

3. Click **Yes** on the Activate Task Confirmation window.
4. The Activate Progress window is displayed. Once Activate is complete, click **OK**.

Appendix G. Customizable data replication

The Customizable Data Replication service provides the ability to configure a set of Hardware Management Consoles to automatically replicate any changes to certain types of data so that the configured set of Hardware Management Consoles automatically keep this data synchronized without manual intervention.

Notes:

- Customizable Data Replication is available only on Hardware Management Consoles at Version code 1.8.0 and later.
- Before enabling this replication service, you may want to save your original data settings in case you need to restore these settings at a future time. See “Save/Restore Customizable Console Data” on page 119.
- The **Configure Data Replication** task and the **Save/Restore Customizable Console Data** task are not supported between Hardware Management Consoles Version 1.x.x and Hardware Management Consoles Version 2.x.x. They are supported when you want to perform these tasks within Version 1.x.x or within Version 2.x.x.

The following types of data can be configured:

- Acceptable Status Settings
 - Any status settings that are considered acceptable for all types of managed objects.
- Associated Activation Profiles
 - Associated activation profile settings for CPC and CPC image objects defined in the **Customize/Delete Activation Profiles** task.
- Customer Information Data
 - Administrator information (customer name, address, telephone number, etc.)
 - System information (administrator address)
 - Account information (customer number, enterprise number, sales branch office, etc.).
- Group Data
 - All user-defined group definitions.
- Modem Configuration Data
 - Configure modem for remote support.
- Monitor System Events Data
 - SMTP server and port setting
 - Minimum time between emails setting
 - Event monitors.
- Object Locking Data
 - Enable automatic locking of objects after they are used as target objects for a task.
- Outbound Connectivity Data
 - Configure local modem to Remote Support Facility (RSF)
 - Enable an internet connection
 - Configure to an External Time Source.
- Remote Service Data
 - Enablement of remote service
 - Enablement of automatic service call
 - Service telephone number configuration.
- User Profile Data
 - Customized user IDs defined in the **User Profiles** task

- Customized user managed resource roles and task roles defined in the **User Profiles** task
- LDAP servers defined in the **Manage Enterprise Directory Server Definitions** task
- Password profile information defined in the **Password Profiles** task
- Logon session properties
- Remote access using a web browser
- All user settings defined in the **User Settings** task:
 - Defining color or gray patterns
 - Any confirmation settings
 - Controls such as displaying hover help, single object selections, or console messaging
 - Defining the user interface style: tree or classic
- Tree style preferences
- LDAP user ID.
- User pattern and user template definitions.
- User settings for synthetic user IDs created using a template definition.

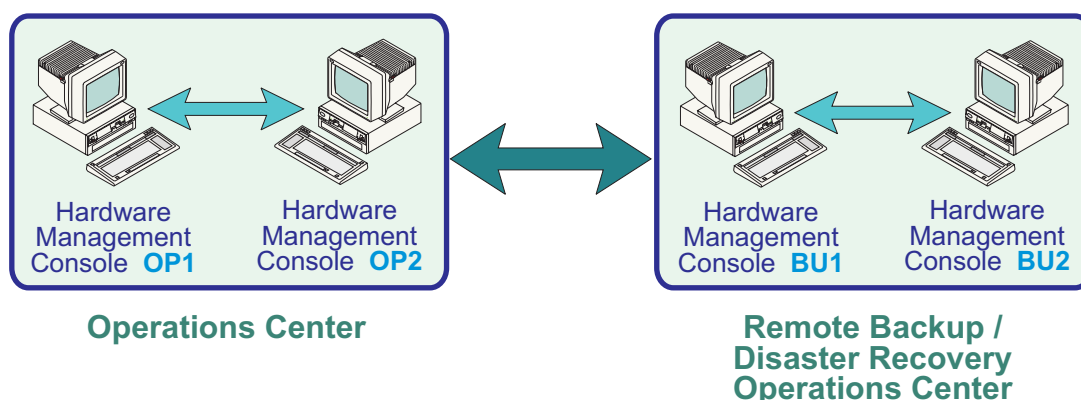
The Customizable Data Replication service can be enabled for the following types of operations:

- **Peer-to-Peer** (see “Example 1: Peer-to-peer replication”)

Provides automatic replication of the selected customized data types between peer Hardware Management Consoles. Changes made on any of these consoles are replicated to the other consoles.
- **Master-to-Slave** (see “Example 2: Master-to-slave replication” on page 246.)

Provides automatic replication of the selected customized data types from one or more designated master Hardware Management Consoles to one or more designated slave Hardware Management Consoles. Changes made on a master(s) console are automatically replicated to the slave console(s).

Example 1: Peer-to-peer replication



1. Log on the Hardware Management Console using the ACSADMIN default user ID or a user ID that has Access Administrator roles.
 2. Open the **Configure Data Replication** task. The Configure Customizable Data Replication window is displayed.
 3. Select **Enable** in the **Configure Data Replication** area.
 4. The Configure Customizable Data Replication window is displayed.
 5. Click **New** under **Data Source(s)**. The Configure New Replication Source window is displayed.
 6. Select a *Hardware Management Console* to be used as a data source from the **Discovered Console Information** list, and click **Add**.
- or
- Enter the *TCP/IP address* of the Hardware Management Console to be used as a data source in the **TCP/IP Address Information** input field, and then click **Find**.

Note: Hardware Management Consoles *must be* at Version code 1.8.0 or later.

- The Configure Customizable Data Replication window is displayed again as shown in Figure 65.

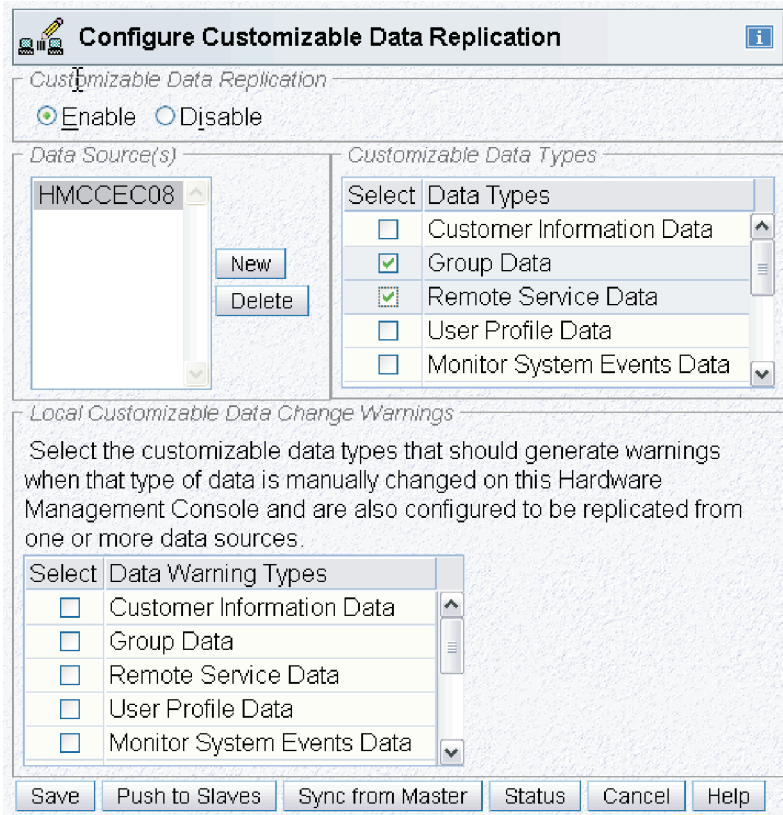
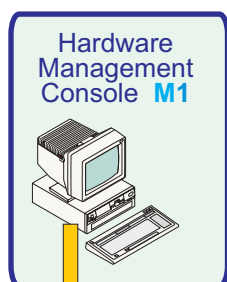


Figure 65. Configure customizable data replication window - example 1

- Select the types of data from the **Customizable Data Types** list that you want to replicate from a peer Hardware Management Console currently selected under **Data Source(s)**.
- Choose one of the following actions:
 - Click **Save** to close the Configure Customizable Data Replication window.
 - Click **Push to Slaves** to transfer all local levels to any communicating slave. The slaves, if they are running this level of code, are instructed to accept the levels from the master, regardless of the value of their current levels.
 - Click **Sync from Master** to invalidate the local levels for all properties that are defined to have a master. This results in an immediate level set where the master(s) provide their levels to the local machine. This option is not available if the local Hardware Management Console is not defined to have any data sources.
 - Click **Status** to show the status of this task on this machine.
- Repeat **steps 1** through **9** on each of the Hardware Management Consoles you want to act as peers with one another.
- Once communication is established between the Hardware Management Consoles, the requested types of customizable data are automatically replicated from one Hardware Management Console to the other immediately following the change in the data itself.

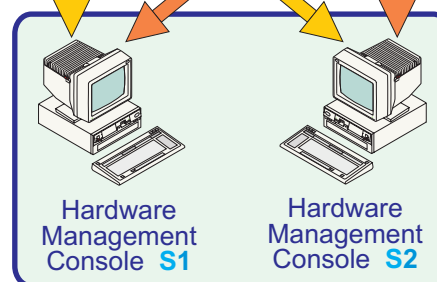
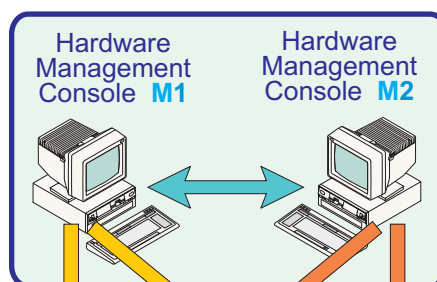
Example 2: Master-to-slave replication

Operations Center



Machine Room

Operations Center



Machine Room

Setting up a Master Console(s):

1. Log on the Hardware Management Console using the ACSADMIN default user ID or a user ID that has Access Administrator roles.
2. Open the **Configure Data Replication** task. The Configure Customizable Data Replication window is displayed.
3. Select **Enable** in the **Customizable Data Replication** area.
4. Click **Save** to close the Configure Customizable Data Replication window.

Note: If you want to configure additional master consoles, see “Example 1: Peer-to-peer replication” on page 244.

Setting up the Slave Console(s):

1. Log on the Hardware Management Console using the ACSADMIN default user ID or a user ID that has Access Administrator roles.
2. Open the **Configure Data Replication** task. The Configure Customizable Data Replication window is displayed.
3. Select **Enable** in the **Customizable Data Replication** area.
4. The Configure Customizable Data Replication window is displayed.
5. Click **New** under **Data Source(s)**. The Configure New Replication Source window is displayed.
6. Select a *Hardware Management Console* to be used as a master data source from the **Discovered Console Information** list, then click **Add**.

or

Enter the *TCP/IP address* of the Hardware Management Console to be used as the master data source in the **TCP/IP Address Information** input field, then click **Find**.

Note: Hardware Management Consoles *must be* at Version code 1.8.0 or later.

- The Configure Customizable Data Replication window is displayed again as shown in Figure 66.

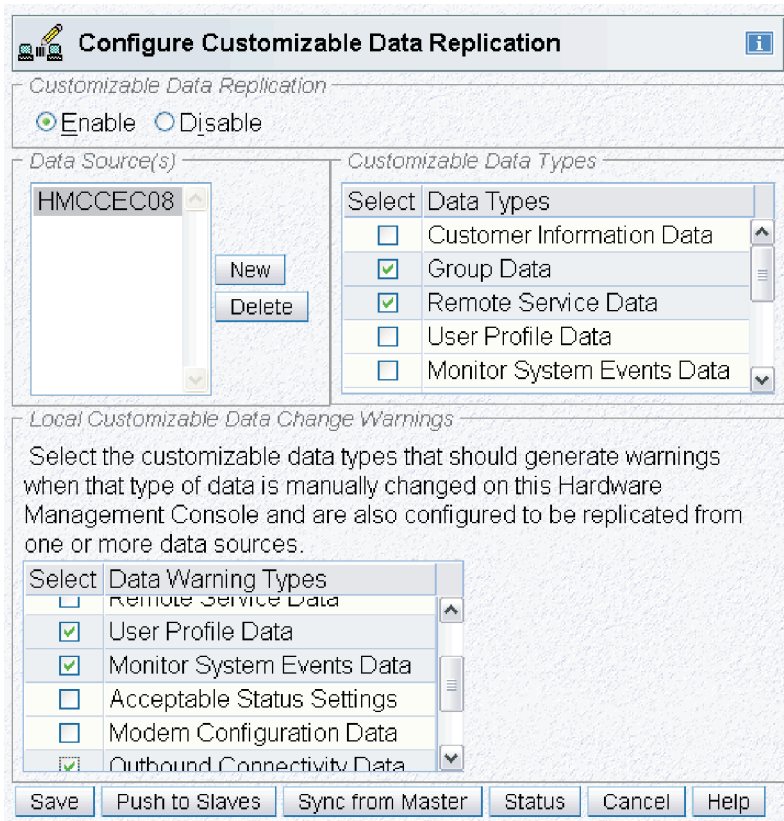


Figure 66. Configure customizable data replication window - example 2

- Select the types of data from the **Customizable Data Types** list that you want to accept from the Hardware Management Console currently selected under **Data Source(s)**.

Note: When configuring a Hardware Management Console as a slave, you should check the types of customizable data from the **Local Customizable Data Change Warnings** list that should generate warnings to a user when manual changes are made to that data on this Hardware Management Console.

- Choose one of the following actions:
 - Click **Save** to close the Configure Customizable Data Replication window.
 - Click **Push to Slaves** to transfer all local levels to any communicating slave. The slaves, if they are running this level of code, are instructed to accept the levels from the master, regardless of the value of their current levels.
 - Click **Sync from Master** to invalidate the local levels for all properties that are defined to have a master. This results in an immediate level set where the master(s) provide their levels to the local machine. This option is not available if the local Hardware Management Console is not defined to have any data sources.
 - Click **Status** to show the status of this task on this machine.
- Repeat **steps 1** through **9** on any additional Hardware Management Consoles that you want to configure as a slave.

11. Once communication is established between all of the Hardware Management Consoles, the master console(s) remains synchronized with each other, providing redundancy in the event that one of the master consoles becomes unavailable. The slave console(s) are kept synchronized with whichever master console provides the data to them first.

Data replication

As data is replicated from one Hardware Management Console to another, an internal level indicator for the data being replicated is incremented each time the data is altered on the data source. Each Hardware Management Console keeps track of the level indicator for each type of data and will not accept data from a data source when the level indicator is not greater than that on the receiving Hardware Management Console.

If for some reason there is a need to force the replication of data from one or more data sources and the level indicator on the receiving Hardware Management Console is greater than that of the data sources, do the following:

1. Log on the Hardware Management Console using the ACSADMIN default user ID or a user ID that has Access Administrator roles.
2. Open the **Configure Data Replication** task. The Configure Customizable Data Replication window is displayed (**Enable** should be selected).
3. Deselect all the data types from the **Customizable Data Types** list on the Configure Customizable Data Replication window.

Note: If you just want to reset the level indicator for a particular data type, just deselect that data type.

4. Click **Save** to remember the changes and to close the Configure Customizable Data Replication window.
5. Start the **Configure Data Replication** task again by repeating **step 2**.
6. Select the types of data from the **Customizable Data Types** list that were just deselected in **step 3**.
7. Click **Save** to remember the changes and to close the Configure Customizable Data Replication window.

Note: Deselecting and then reselecting the data types resets the internal level indicators for the specified types of data and forces replication of the data from the data sources.

Appendix H. Installing software from a mass storage device

This appendix describes the procedure for installing an operating system (such as, Linux or z/VM) from a mass storage device to your system processor that does not have a CD or DVD drive attached to it. Using the **Enable FTP Access to Mass Storage Media** task, the **Load from Removable Media or Server** Recovery task, and monitoring the **Operating System Messages** will assist you in accessing this software.

Before you begin, you need to know the IP addresses of the following:

- The system processor you want to install the software on.
- The Hardware Management Console you will be getting the software from.

To locate this IP Address:

1. Open the **Customize Network Settings** task. The Customize Network Settings window is displayed.
2. Select **LAN Adapters** tab. The **LAN Adapters** table is displayed. From the list of LAN adapters, note the IP address of the network adapter that connects the processor to the Hardware Management Console.

Perform the following Hardware Management Console steps:

1. If you have not already done so, log on to the Hardware Management Console using the SYSPROG default user ID or a user ID that has been assigned System Programmer roles.
 2. Insert the media that contains the operating system you want installed on your processor.
 3. Open the group of defined CPCs that contains the object with the Support Element that you want to connect to.
 4. Select one CPC.
 5. Open the group of defined CPC images that contains the image that you want to connect to.
 6. Open the **Load from Removable Media or Server** Recovery task to start it. The Load from Removable Media or Server Task Confirmation window is displayed.
 7. Click **Yes** to continue. The Load from Removable Media or Server window is displayed.
 8. Select **Hardware Management Console CD-ROM / DVD** and specify a **File location** as required for your load media on the Load from Removable Media or Server window.
 9. Click **OK** and perform the operation.
 10. Open the **Enable FTP Access to Removable Mass Storage Media** task. The Enable FTP Access to Mass Storage Media message window is displayed. To allow FTP access to the mass storage media, click **Yes**.
 11. The Enable FTP Access to Removable Mass Storage Media window is displayed.
 12. Specify the TCP/IP address of the processor that you want the software to be sent to, then click **Enable**. The **Enable FTP Access to Mass Storage Media** message window is displayed. Minimize this window, you will need the information in step 10.
 13. Use **Operating System Messages** or the appropriate interface to continue the loading.
 14. Click **OK** to close the window when installation is complete.
- or
- a. Click **Exchange Media** on the Enable FTP to Mass Storage Media window to insert the next media.
 - b. Repeat step a until all media has been read, then click **CLOSE** on the Enable FTP to Mass Storage Media window when you are finished.

Appendix I. Notices

This information was developed for products and services offered in the USA.

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
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](http://www.ibm.com)® are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at <http://www.ibm.com/legal/copytrade.shtml>.

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

InfiniBand is a registered trademark of the InfiniBand Trade Association.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other product and service names might be trademarks of IBM or other companies.

Electronic emission notices

The following 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 instructions contained in the installation 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, by installation or use of this equipment other than as specified in

the installation manual, or by any other 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.

Canadian Department of Communications Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité aux normes du ministère des Communications du Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

European Union (EU) Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC 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 55022. The limits for Class equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

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.

European Community contact:

IBM Technical Regulations
Pascalstr. 100, Stuttgart, Germany 70569
Telephone: 0049 (0) 711 785 1176
Fax: 0049 (0) 711 785 1283
email: tjahn@de.ibm.com

EC Declaration of Conformity (In German)

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 89/336/EWG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 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 der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 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 89/336/EWG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) vom 18. September 1998 (bzw. der EMC EG Richtlinie 89/336) für Geräte der Klasse A.

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Konformitätserklärung nach Paragraph 5 des EMVG ist die IBM Deutschland GmbH, 70548 Stuttgart.

Informationen in Hinsicht EMVG Paragraph 4 Abs. (1) 4:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

update: 2004/12/07

People's Republic of China Class A Compliance Statement

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 actions.

声 明

此为 A 级产品,在生活环境中,
该产品可能会造成无线电干扰。
在这种情况下,可能需要用户对其
干扰采取切实可行的措施。

Japan Class A Compliance Statement

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.

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用する
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

Korean Class A Compliance Statement

이 기기는 업무용(A급)으로 전자파적합등록을 한 기기이오니
판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의
지역에서 사용하는 것을 목적으로 합니다.

Taiwan Class A Compliance Statement

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user will be required to take adequate measures.

警告使用者：
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

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

Index

Numerics

3270

- emulators, configuring 86
- integrated console 145

A

- acceptable status 55
- access removable media task 144
- activate option 211
- activate task 9, 138, 194
- activation of an upgrade
 - phases
 - completion 212
 - preparation 212
 - transition 212
- activation profiles 8
 - See* customize/delete activation profiles task
- active tasks
 - fibre channel network 67
 - hardware management console 66
 - optical network 66
 - user-defined groups 28, 66
- activity profiles, customize 192
- activity task 191
- add object definition for undefined
 - director/timer consoles 181
- add object definition task 181, 216
- add object definition using
 - CPC manual definition 29, 64
 - director/timer console manual definition template 181
 - fiber saver manual definition template 29, 65
- addresses
 - server
 - ip 226
- advanced facilities, OSA 178
- alternate support element
 - switching 160
- alternate support element engineering
 - changes (ECs) task 161
- alternate support element task 159
- analyze console internal code task 81
- API settings, customizing 90
- arbiter 236
- archive security logs
 - for a hardware management console 82
- archive security logs task
 - for a CPC 152
- ASCII, integrated console 145
- audit and log management task 82
- authorize internal code changes task 82
- automatic activation task 171

B

- backing up critical data
 - hardware management console 83
 - support element 153
- backup critical console data task 83
- backup critical data task 153
- backup time server 236
- banner 15
- basic mode xiii
- block automatic licensed internal code
 - change installation task 84
- books, online 79
- broadcast message 88
- broadcast messages 94
- browser 215
 - remote operation 93
 - remote restart 93
- busy objects 53

C

- call-home server consoles 97
- call-home servers 226
- certificate management task 84
- change console internal code task 85
- change features xv
- change internal code task 162
- change LPAR
 - I/O priority queuing task 173
- change LPAR controls task 172
- change LPAR group controls task 173
- change LPAR I/O priority queuing task 173
- change management 93
 - alternate support element 159
 - alternate support element engineering
 - changes (ECs) 161
 - change internal code 162
 - concurrent upgrade engineering
 - changes (ECs) 162
 - engineering changes (ECs) 163
 - hardware messages 77
 - help 80
 - operating system messages 78
 - product engineering directed
 - changes 164
 - retrieve internal code 164
 - save legacy upgrade data 165
 - single step internal code changes 166
 - special code load 167
 - system information 168
- change management tasks 159
 - alternate support element 159
 - change internal code 162
 - engineering changes 163
 - product engineering directed
 - changes 164
 - retrieve internal code 165
 - single step internal code changes 166
 - special code load 168

change management tasks (*continued*)

- system information 168
- change object definition task 182
- change password task 85
- changing
 - default colors for processor status changes 127
- changing interface styles 4
- changing time-of-day clock
 - setting the hardware management console date and time 239
 - setting the support element time
 - time source enabled 240
 - time source not enabled 240
 - setting the support element time zone 239
- channel paths
 - configuring on/off 174
 - reassigning 179
- choose z/VM virtual machines to manage task 195
- CIM (common information model) 90, 94
- CIM management interface 90, 94
- classic interface 2, 47, 48
 - degraded message under CPC
 - icon 62
 - groups 59
 - hover help 48
 - messages
 - service required 62
 - resize workplace 47
 - settings
 - chat window 127
 - colors 127
 - console messenger 127
 - hover help 127
 - patterns 127
 - show tips 127
 - single object selection 127
 - workplace, hardware management console 6
 - monitoring your hardware 55
 - opening an object 49
 - performing a task 52
 - selecting objects 48
 - unacceptable status 55
- colors 127
- common information model (CIM) 90, 94
- completion 212
- completion phase 212
- components of the tree style user interface 15
- concurrent upgrade engineering changes (CUEC) 209
 - activate 211
 - preload 210
 - query function availability from last
 - activate 213
 - switch points 209

- concurrent upgrade engineering changes (CUEC) *(continued)*
 - task 209
- concurrent upgrade engineering changes (ECs) task 162, 209
- preload options 211
- configuration 31
 - edit frame layout 184
 - ETR 232
 - hardware messages 77
 - help 80
 - operating system messages 78
 - STP 232
 - system (sysplex) time 229
 - transmit vital product data 122
- configuration tasks 184
 - edit frame layout 184
 - input/output configuration save and restore 184
 - system (sysplex) time 186
 - system input/output configuration analyzer 185
 - transmit vital product data 186
 - view frame layout 187
- configure channel path on/off task 174
- configure data replication task 86, 243
- configuring an NTP server 92
- configuring for
 - a 3270 emulator session 86
- confirmation windows 126
- connecting to
 - web browser 215
- connectivity
 - remote support facility 223, 224
 - proxy SSL 225
 - SSL 225
- console actions 81
 - analyze console internal code 81
 - archive security logs 82
 - audit and log management 82
 - authorize internal code changes 82
 - backup critical console data 83
 - block automatic licensed internal code
 - change installation 84
 - certificate management 84
 - change console internal code 85
 - change password 85
 - configure 3270 emulators 86
 - console default user settings 87
 - console messenger 87
 - create welcome text 89
 - customize automatic logon 91
 - customize console date/time 91
 - customize console services 93
 - customize customer information 94
 - customize modem settings 95
 - customize network settings 95
 - customize outbound connectivity 97
 - customize product engineering access 99
 - customize remote service 100
 - customize scheduled operations 100
 - customize user controls 102
 - domain security 103
 - enable electronic service agent 103
 - enable FTP access to mass storage media 105
- console actions *(continued)*
 - fibre channel analyzer 105
 - format media 106
 - hardware management console
 - settings 106
 - installation complete report 108
 - logoff or disconnect 108
 - manage enterprise directory server definitions 109
 - manage print screen files 109
 - manage remote connections 110
 - manage remote support requests 111
 - manage SSH keys 111
 - manage users wizard 111
 - manage web services API 112
 - monitor system events 112, 192
 - network diagnostic information 113
 - object locking settings 114
 - offload virtual RETAIN data to removable media 115
 - password profiles 115
 - perform a console repair action 115
 - reassign hardware management console 116
 - rebuild vital product data 116
 - remote Hardware Management Console 117
 - report a problem 117
 - restore legacy HMC data 118
 - save upgrade data 118
 - save/restore customizable console data 119
 - shutdown or restart 120
 - single step console internal code changes 121
 - tip of the day 122
 - transmit console service data 122
 - transmit vital product data 122
 - user patterns 123
 - user profiles 123, 124, 129
 - user settings 126
 - user templates 129
 - users and tasks 130
 - view console events 130
 - view console information 131
 - view console service history 132
 - view console tasks performed 132
 - view licenses 132
 - view only 102
 - view PVM records 133, 156
 - view security logs 134
 - what's new 134
- console default user settings task 87
- console messenger 94
- console messenger task 87
 - broadcast message 88
 - two-way chat 88
- coordinated server time (CST) 236
- coordinated timing network (CTN) 236
- coordinated timing network identifier (CTN ID) 236
- copy console logs to media task 89
 - copy console logs to media 89
- CPC details 9, 50, 55
- zBX option 52
- CPC images 60
- CPC manual definition
 - introduction 29, 64
 - TCP/IP 64
- CPCs
 - defined 61
 - details 55
 - undefined 28, 64
- create welcome text task 89
- CTN
 - mixed
 - STP-only 229
- current time server 236
- custom groups 28
- customer information task 169
- customizable data replication 243
 - master-to-slave 244
 - peer-to-peer 244
- customize
 - activity profiles 192
 - API settings task 90
 - auto answer settings task 91
 - automatic logon task 91
 - console date/time task 91
 - console services task 93
 - customer information task 94
 - delete activation profiles task 174
 - modem settings task 95
 - network settings task 95
 - outbound connectivity task 97
 - product engineering access task 99
 - remote service task 100
 - scheduled operations task
 - console 100
 - cpc 175
 - support element date/time task 177
 - user controls task 102
- customize activity profiles 192
- customize API settings
 - CIM management interface 90
- customize API settings task 90
- customize auto answer settings 91
- customize automatic logon task 91
- customize console date/time task 91, 239
- customize console services task 93
 - CIM management interface 94
 - console messenger 94
 - fibre channel analysis 94
 - large retrieves from RETAIN 94
 - LIC change 93
 - optical error analysis 93
 - remote operation 93
 - remote restart 93
- customize customer information task 94
- customize network settings task 249
- customize product engineering access task 99
- customize remote service task
 - zBX option 100
- customize scheduled operations task
 - console 100
 - cpc 175
- customize support element date/time task 177
- customize user controls task 203
- customize/delete activation profiles task 174

D

- daily tasks 138
 - activate 138
 - deactivate 139
 - grouping 140
 - hardware messages 77
 - help 80
 - operating system messages 78
 - reset normal 142
- data replication 248
 - configuring 86
 - customizable 243
 - grouping task 140
- deactivate task 139, 195
- default
 - user roles 12
- default profile 8
- default user IDs 203
- default user IDs and passwords 12
- defined
 - CPCs 61
 - director/timer consoles 27, 63
 - fiber savers 27, 63
- defining
 - directors/timers
 - using tree user interface 29
 - fiber savers
 - using tree user interface 29
 - systems
 - using tree user interface 28
- defining undefined director/timer consoles 181
- defining undefined fiber savers 29, 65
- defining user roles
 - See* user profiles task
- details
 - displaying for CPC or image 50
- details window 51
- dial prefix 95
- dial tone 95
- dial type 95
- direct manipulation 52
- director/timer console manual definition
 - template 29, 65
- director/timer consoles 27, 63
- disabling
 - CIM management interface 90, 94
 - console messenger 94
 - console services 93
 - CIM management interface 94
 - console messenger 94
 - fiber channel analysis 94
 - large retrieves from RETAIN 94
 - LIC change 93
 - optical error analysis 93
 - remote operation 93
 - remote restart 93
 - fiber channel analysis 94
 - large retrieves from RETAIN 94
 - LIC change 93
 - optical error analysis 93
 - remote operation 93
 - remote restart 93
 - SNMP 90
- disruptive tasks 6
 - activate 138
 - change internal code 162

- disruptive tasks (*continued*)
 - configure channel path on/off 174
 - deactivate 139
 - engineering changes 163
 - load 146
 - product engineering directed changes 164
 - PSW restart 147, 148, 186
 - reboot support element 182
 - reset clear 148
 - reset normal 142, 149
 - single step internal code changes 166
 - special code load 168
 - system (sysplex) time 186
- domain security task 103

E

- edit frame layout task 184
- edit the VMRM active configuration file
 - task 196
- emulator sessions, configuring for a 3270 86
- enable electronic service agent task 103
- enable ftp access to mass storage media task 249
- enable FTP access to mass storage media task 105
- enable I/O priority queuing task 177
- enabling
 - CIM management interface 90, 94
 - console messenger 94
 - console services 93
 - CIM management interface 94
 - console messenger 94
 - fiber channel analysis 94
 - large retrieves from RETAIN 94
 - LIC change 93
 - optical error analysis 93
 - remote operation 93
 - remote restart 93
 - fiber channel analysis 94
 - hardware management console
 - application program interface (API) 127
 - I/O priority queuing task 177
 - large retrieves from RETAIN 94
 - LIC change 93
 - optical error analysis 93
 - remote operation 93
 - remote restart 93
 - SNMP 90
- energy management tasks 188
 - set power cap 188
 - set power saving 188
- engineering changes (ECs) task 163
- engineering changes task 163
- enhanced driver maintenance 209
 - switch points 209
- ensemble management 30
- environmental efficiency statistics
 - data 190
- environmental efficiency statistics task 190
- ETR configuration 232
- ETR feature 229
- ETR network 236

- ETR network ID 236
- ETR status 232
- ETR timing mode 237
- event monitor 112, 192
- exceptions 70
- external time reference (ETR) 240
- external time source 99
- External Time Source (ETS) 237

F

- feature
 - ETR 229
- features
 - changed xv
 - new xv
 - topology 41
- fenced internet 224
- fiber saver manual definition
 - template 29, 65
- fiber channel analysis 94
- fiber channel analyzer 105
- fiber channel network 60, 67
- format
 - web address 218
- format media task 106

G

- graphical user interface 215
- group profile 8
- grouping task 140, 196
 - pattern match group 140, 196
- groups 59
 - CPC images 60
 - defined CPCs 61
 - defined director/time consoles 27
 - defined director/timer consoles 63
 - defined fiber savers 27, 63
 - fiber channel network 60
 - hardware management console 60
 - optical network and system I/O 60
 - undefined CPCs 28, 64
 - undefined director/timer consoles 29, 65
 - undefined fiber savers 29, 65
 - user-defined 28, 66

H

- hardware management console
 - logging on 11, 12
 - starting 11
- hardware management console settings
 - configure data replication task 86
 - customize API settings task 90
 - customize automatic logon settings task 91
 - customize console services task 93
 - customize customer settings task 95
 - customize modem settings task 95
 - customize network settings task 95
 - customize outbound connectivity task 97
 - customize product engineering access task 99

- hardware management console settings (continued)
 - customize remote service task 100
 - HMC management tasks
 - customize automatic logon 91
 - customize product engineering access 99
 - object locking settings task 114
- hardware management console settings task 106
- hardware management console web browser
 - getting ready to use 219
 - introduction 217
 - requirements 218
- hardware messages 44, 77
- help, online 80
- HMC management 30
 - alphabetical listing
 - categorized list 30
 - configuration 31
 - tasks 30
- HMC management tasks 81
 - archive security logs 82
 - backup critical console data 83
 - certificate management 84
 - change password 85
 - configure 3270 emulators 86
 - configure data replication 86
 - console default user settings 87
 - console messenger 87
 - create welcome text 89
 - customize API settings 90
 - customize console date/time 91
 - customize console services 93
 - customize customer information 94
 - customize scheduled operations 100
 - customize user controls 102
 - customize user controls task 102
 - domain security 103
 - enable ftp access to mass storage media 105
 - format media 106
 - manage enterprise directory server definitions 109
 - manage print screen files 109
 - manage web services API 112
 - monitor system events 112
 - network diagnostic information 113
 - object locking settings 114
 - offload virtual RETAIN data to removable media 115
 - password profiles 115
 - reassign hardware management console 116
 - remote Hardware Management Console 117
 - save upgrade data 118
 - save/restore customizable console data 119
 - shutdown or restart 120
 - tip of the day 122
 - user settings 126
 - users and tasks 130
 - view console events 130
 - view console information 131
 - view licenses 132

- HMC management tasks (continued)
 - view PMV records 133, 156
 - view security logs 134
 - what's new 134
- hover help 48
- html version of guide xiv

I

- image details 9, 50
- image profile 8
- initial microcode load (IML) 138, 194
- initial program load (IPL) 138, 194
- input/output configuration save and restore task 184
- installation complete report task 108
- installing
 - software from a mass storage device 249
- instant messages 94
- instant messaging 87
 - console default user settings task 87
 - console messenger task 87
 - customize console services task 93
 - user settings task 126, 127
 - users and tasks task 130
- integrated 3270 console task 145
- integrated ASCII console task 145
- interfaces
 - classic 2, 47
 - tree 2, 15
- internet connectivity 224
- ip addresses 226
- IPv6 4

L

- large retrieves from RETAIN 94
- LIC change 93
- lightweight directory access protocol (LDAP) 4
- load address 138, 194
- load from removable media or server task 147, 249
- load profile 8
- load task 146
- local timing mode 237
- locking disruptive tasks 6
- logging on to the hardware management console 11
- logging on to the Hardware Management Console 12
- logical processor add task 178
- logical processor assignment 172
- logically partitioned (LPAR) mode xiii
- logoff or disconnect task 108
- LPAR controls, changing 172

M

- maintain z/VM profiles task 198
- maintain z/VM prototypes task 198
- maintain z/VM virtual machines to manage task 199
- maintain z/VM volume space task 200

- manage enterprise directory server definitions task 109
- manage print screen files task 109
- manage remote connections task 110
- manage remote support requests task 111
- manage SSH keys task 111
- manage users wizard task 111
- manage web services API task 112
- managing user roles
 - See customize user controls task
- manual definition 29, 64
- mass storage device
 - installing software 249
- memory key
 - See USB flash memory drive
- messages
 - degraded 62
 - hardware 77
 - operating system 78
- mirroring support element data 159
- mixed coordinated timing network (mixed CTN) 237
- mixed CTN 229
- modem connectivity 223
- modem settings, customizing 95
- monitor
 - environmental efficiency
 - statistics 190
 - monitors dashboard task
 - activity 191
- monitor dashboard task
 - customize activity profiles 192
- monitor system events task 112, 192
- monitor tasks 190
 - environmental efficiency
 - statistics 190
 - monitor system events 192
 - monitors dashboard 190
- monitors 112, 192
- monitors dashboard task 190
 - activity 191

N

- navigation pane 15
- network configuration 231
- network diagnostic information task 113
- Network Time Protocol (NTP) 237
- new features xv
- nodes
 - systems 19
- NTP (network time protocol) 237
- NTP server configuration 92

O

- object definition
 - add object definition 181
 - change object definition 182
 - CPC manual definition 29, 64
 - hardware messages 77
 - help 80
 - operating system messages 78
 - reboot support element 182
 - remove object definition 183

- object definition tasks 181
 - add object definition 181
 - change object definition 182
 - reboot support element 182
 - remove object definition 183
- object locking for disruptive tasks 6, 45
- object locking settings task 45, 114
- objects
 - opening 49
 - selecting 48
- offload virtual RETAIN data to removable media task 115
- online books 79
- online help 48, 80
- opening tasks
 - context menu 23
 - tasks menu 24
 - tasks pad 21
 - using the tree interface 21
- operating system messages 44, 78
- operational customization
 - automatic activation 171
 - change LPAR controls 172
 - change LPAR I/O priority queuing 173
 - configure channel path on/off 174
 - customize scheduled operations 175
 - customize support element date/time 177
 - customize/delete activation profiles 174
 - enable I/O priority queuing 177
 - hardware messages 77
 - help 80
 - logical processor add 178
 - operating system messages 78
 - OSA advanced facilities 178
 - reassign channel path 179
 - view activation profiles 180
- operational customization tasks 171
 - automatic activation 171
 - change LPAR controls 172
 - change LPAR group controls 173
 - change LPAR I/O priority queuing 173
 - configure channel path on/off 174
 - customize scheduled operations 175
 - customize support element date/time 177
 - customize/delete activation profiles 174
 - enable I/O priority queuing 177
 - logical processor add 178
 - OSA advanced facilities 178
 - reassign channel path 179
 - view activation profiles 180
- operations
 - remote 215
- optical error analysis 93
- optical network 66
- optical network and system I/O 60
- options
 - activate 211
 - preload 210
 - query function availability from last activate 213
 - zBX 52, 100, 156, 170

OSA advanced facilities task 178

P

- password
 - changing 85
- password profiles task 115
- passwords and user IDs
 - default 12
- pattern match group 140, 196
- patterns 127
- pdf version of guide xiv
- perform a console repair action task 115
- perform problem analysis task 153
- perform transfer rate test task 154
- PPS control 235
- predefined user IDs 203
- preferred time server 237
- preload 210
- preload options 211
- preparation 212
- preparation phase 212
- problems
 - fibre channel analysis 94
 - large retrieves from RETAIN 94
 - optical error analysis 93
- processor running time 172
- product engineering directed changes task 164
- profiles
 - activation 8
 - customize activity 192
 - customize/delete activation 174
 - default 8
 - group 8
 - image 8
 - load 8
 - reset 8
 - view activation 180
- proxy SSL connection 225
- PSW restart task 148

Q

- query function availability from last activate 213
- querying switch capability 160

R

- reassign channel path task 179
- reassign hardware management console task 116
- reboot support element task 182
- rebuild vital product data task 116
- receiving a broadcast message 88
- recovery
 - access removable media 144
 - hardware messages 77
 - help 80
 - integrated 3270 console 145
 - integrated ASCII console 145
 - load 146
 - operating system messages 78
 - PSW restart 148
 - reset clear 148

recovery (*continued*)

- reset normal 149
- single object operations 149
- start all 150
- stop all 151
- recovery tasks 144
 - integrated ASCII console 145
 - load 146
 - load from removable media or server 147
 - PSW restart 148
 - reset clear 148
 - reset normal 149
 - single object operations 149
 - start all 150
 - stop all 151
- remote customization
 - customer information 169
 - hardware messages 77
 - help 80
 - operating system messages 78
 - remote service 169
 - support element operations guide 170
- remote customization tasks 169
 - customer information 169
 - remote service 169
 - support element operations guide 170
- remote hardware management console TCP/IP 64
- remote Hardware Management Console task 117
- remote operation 93, 215
- remote restart 93
- remote service task 169
 - zBX option 170
- remote support facility (RSF) 223
 - connectivity 223
 - internet 224
 - modem 223
 - proxy SSL connection 225
 - SSL connection 225
- remove object definition task 183
- replication
 - customizable data 243
- report a problem task 154
 - hardware management console 117
 - support element 154
- requirements
 - web browser 218
- reset
 - normal task, recovery 149
- reset clear task 148
- reset normal task 142, 149
- reset profile 8
- resizing panes using tree style user interface 16
- resizing workplace 47
- restart 120
- restore critical data task 155
- restore legacy HMC data task 118
- retrieve internal code task 164, 165

S

- SAD (system activity display) 191
- save legacy upgrade data task 165
- save upgrade data task 118
- save/restore customizable console data task 119, 243
- selecting objects
 - tasks 137
- sending a message 87
- sending messages 94
- server addresses 226
- server time protocol (STP) 186, 229, 240
- servers
 - call-home 226
- service
 - archive security logs 152
 - backup critical data 153
 - hardware messages 77
 - help 80
 - operating system messages 78
 - perform problem analysis 153
 - perform transfer rate test 154
 - report a problem 154
 - restore critical data 155
 - service status 155
 - transmit service data 156
 - view service history 157
- service management 32
 - alphabetical listing
 - categorized list 32
 - perform a console repair action 115
 - tasks 32
- service management tasks 81
 - analyze console internal code 81
 - authorize internal code changes 82
 - block automatic microcode installation 84
 - change console internal code 85
 - customize auto answer settings 91
 - customize modem settings 95
 - customize outbound connectivity 97
 - customize remote service 100
 - enable electronic service agent 103
 - fibre channel analyzer 105
 - installation complete report task 108
 - manage remote connections 110
 - manage remote support requests 111
 - rebuild vital product data 116
 - report a problem 117
 - restore legacy HMC data 118
 - single step console internal code 121
 - transmit console service data 122
 - transmit vital product data 122
 - view console service history 132
 - view console tasks performed 132
- service required message 62
- service status task 155
- service tasks 152
 - archive security logs 152
 - backup critical data 153
 - perform problem analysis 153
 - perform transfer rate test 154
 - report a problem 154
 - restore critical data 155
 - service status 155
 - transmit service data 156
 - view service history 157
- services
 - customizing 93
 - CIM management interface 90, 94
 - console messenger 94
 - fibre channel analysis 94
 - large retrieves from RETAIN 94
 - LIC change 93
 - optical error analysis 93
 - remote operation 93
 - remote restart 93
 - enabling 93
 - set power cap task 188
 - set power saving 188
 - setting the user interface
 - See user settings task
 - setting up
 - CIM management interface 90, 94
 - console messenger 94
 - fibre channel analysis 94
 - large retrieves from RETAIN 94
 - LIC change 93
 - optical error analysis 93
 - remote operation 93
 - remote restart 93
 - SNMP 90
 - settings
 - colors 127
 - confirmations 126
 - controls 126, 127
 - patterns 127
 - tree style 126
 - ui style 126, 127
 - shutdown or restart task 120
 - single object operations task 149, 239
 - single step console internal code changes task 121
 - single step internal code changes task 166
 - SMTP server 112
 - SNMP 90
 - speaker, enabling 95
 - special code load task 167, 168
 - SSL connection 225
 - start all task 150
 - starting the hardware management console 11
 - status
 - acceptable 55
 - degraded 62
 - ETR 232
 - service required 62
 - STP 232
 - unacceptable 55
 - status bar 15, 44
 - stop all task 151
 - STP 229
 - terminology 236
 - arbitrator 236
 - backup time server 236
 - coordinated server time 236
 - coordinated timing network 236
 - coordinated timing network identifier (CTN ID) 236
 - current time server 236
 - ETR network 236
 - ETR network ID 236
 - ETR timing mode 237
- STP (continued)
 - terminology (continued)
 - External Time Source (ETS) 237
 - local timing mode 237
 - mixed coordinated timing network (mixed CTN) 237
 - Network Time Protocol (NTP) 237
 - preferred time server 237
 - STP network ID 237
 - STP timing mode 237
 - STP-only coordinated timing network (STP-only CTN) 237
 - stratum 237
 - stratum 0 level 237
 - stratum 1 server 237
 - stratum 2 server 237
 - stratum 3 server 237
 - STP configuration 232
 - STP network ID 237
 - STP status 232
 - STP timing mode 237
 - STP-only coordinated timing network 237
 - STP-only CTN 229
 - stratum 237
 - stratum 0 level 237
 - stratum 1 server 237
 - stratum 2 server 237
 - stratum 3 server 237
 - support element
 - alternate 159
 - mirroring 159
 - operations guide task 170
 - rebooting 182
 - support element operations guide task 170
 - supported processors xiii
 - switch points 209
 - switching to
 - alternate support element 160
 - sysplex timer 186, 229, 240
 - system (sysplex) time task 186, 229
 - ETR configuration 232
 - ETR status 232
 - ETS configuration 233
 - network configuration 231
 - PPS control 235
 - STP configuration 232
 - STP status 232
 - timing network 230
 - system activity display (SAD) 191
 - system events, monitoring 112, 192
 - system information task 168
 - system input/output configuration analyzer task 185
 - systems management 19
 - tasks 19, 137
 - systems management tasks 137
 - change management 159
 - alternate support element 159
 - alternate support element engineering changes 161
 - concurrent upgrade engineering changes 162
 - engineering changes 163

systems management tasks *(continued)*

- change management *(continued)*
 - product engineering directed changes 164
 - single step internal code changes 166
 - special code load 168
 - system information 168
- configuration 184
 - edit frame layout 184
 - input/output configuration save and restore 184
 - system (sysplex) time 186
 - system input/output configuration analyzer 185
 - transmit vital product data 186
 - view frame layout 187
- daily 138
 - activate 138
 - deactivate 139
 - grouping 140
 - reset normal 142
- energy management 188
 - set power cap 188
 - set power saving 188
- monitor 190
 - customize activity profiles 192
 - environmental efficiency statistics 190
 - monitor dashboard 190
 - monitor system events 192
- object definition 181
 - add object definition 181
 - change object definition 182
 - reboot support element 182
 - remove object definition 183
- operational customization 171
 - automatic activation 171
 - change lpar controls 172
 - change LPAR controls 172
 - change LPAR group controls 173
 - change LPAR I/O priority queuing 173
 - configure channel path on/off 174
 - customize scheduled operations 175
 - customize support element date/time 177
 - customize/delete activation profiles 174
 - enable I/O priority queuing 177
 - logical processor add 178
 - OSA advanced facilities 178
 - reassign channel path 179
 - view activation profiles 180
- recovery 144
 - access removable media 144
 - integrated 3270 console 145
 - integrated ASCII console 145
 - load 146
 - load from removable media or server 147
 - PSW restart 148
 - reset clear 148
 - reset normal 149
 - single object operations 149

systems management tasks *(continued)*

- recovery *(continued)*
 - start all 150
 - stop all 151
- remote customization 169
 - customer information 169
 - remote service 169
 - support element operations guide 170
- service 152
 - archive security logs 152
 - backup critical data 153
 - perform problem analysis 153
 - perform transfer rate test 154
 - report a problem 154
 - restore critical data 155
 - service status 155
 - transmit service data 156
 - view service history 157
- z/VM virtual machine management 194
 - activate 194
 - choose z/VM virtual machines to manage 195
 - deactivate 195
 - edit the VMRM active configuration file 196
 - grouping 196
 - maintain z/VM profiles 198
 - maintain z/VM prototypes 198
 - maintain z/VM virtual machines to manage 199
 - maintain z/VM volume space 200
 - undefine z/VM virtual machines for management 200
 - view the VMRM measurement data 200
- z/VM virtual network information 201

T

- table view 36
- tables
 - collapsing resources 39
 - expanding resources 39
 - filtering 40
 - selecting rows 39
- task bar 15
- task list work area 76
- tasks 139, 194, 203
 - change management 159
 - alternate support element 159
 - alternate support element engineering changes 161
 - change internal code 162
 - concurrent upgrade engineering changes 162
 - engineering changes 163
 - product engineering directed changes 164
 - retrieve internal code 165
 - single step internal code changes 166
 - special code load 168
 - system information 168

tasks *(continued)*

- configuration 184
 - edit frame layout 184
 - system (sysplex) time 186
 - system input/output configuration analyzer 185
 - transmit vital product data 186
 - view frame layout 187
- daily 138
 - grouping 140
 - reset normal 142
- energy management 188
- HMC management 30
- monitor 190
 - customize activity profiles 192
 - environmental efficiency statistics 190
 - monitor dashboard 190
- object definition 181
 - add object definition 181
 - change object definition 182
 - reboot support element 182
 - remove object definition 183
- operational customization 171
 - automatic activation 171
 - change LPAR controls 172
 - change LPAR group controls 173
 - change LPAR I/O priority queuing 173
 - configure channel path on/off 174
 - customize scheduled operations 175
 - customize support element date/time 177
 - customize/delete activation profiles 174
 - enable I/O priority queuing 177
 - logical processor add 178
 - OSA advanced facilities 178
 - reassign channel path 179
 - view activation profiles 180
- recovery 144
 - integrated ASCII console 145
 - load 146
 - load from removable media or server 147
 - PSW restart 148
 - reset clear 148
 - reset normal 149
 - single object operations 149
 - start all 150
 - stop all 151
- recoveryintegrated 3270 console 145
- remote customization 169
 - customer information 169
 - remote service 169
 - support element operations guide 170
- service 152
 - backup critical data 153
 - perform problem analysis 153
 - report a problem 154
 - restore critical data 155
 - service status 155
 - transmit service data 156
 - view service history 157

- tasks (*continued*)
 - service management 32
 - servicearchive security logs 152
 - systems management 137
 - z/VM virtual machine management 194
 - deactivate 195
 - grouping 196
- tasks index 34
- TCP/IP Version 6 4
- terminology
 - STP 236
- testing problem reporting on a hardware management console 117
- testing problem reporting on a support element 154
- time source
 - ETR 240
 - STP 240
- time synchronization 239
- time-of-day clock, changing 239
- timing network 230
- tip of the day task 122
- topology view 41
- transition 212
- transition phase 212
- transmit console service data task 122
- transmit service data task 156
 - zBX option 156
- transmit vital product data task (console) 122
- transmit vital product data task (cpc) 186
- tree interface 2, 15, 19, 28
 - components
 - banner 15
 - navigation pane 15
 - status bar 15
 - task bar 15
 - work pane 15
 - CPC manual definition 29
 - custom groups 28
 - directors/timers 27
 - disruptive tasks 45
 - ensemble management 30
 - fiber savers 27
 - HMC management 30
 - opening tasks 21
 - context menu 23
 - tasks menu 24
 - tasks pad 21
 - resizing the panes 16
 - service management 32
 - settings
 - all images 126
 - all objects 126
 - banner 126
 - chat window 126
 - confirmations 126
 - console messenger 126
 - navigation icons 126
 - object list 126
 - show tips 126
 - single object selection 126
 - tasks pad 126
 - work pane icons 126
 - status bar 44

- tree interface (*continued*)
 - status exception 44
 - status hardware messages 44
 - status operating system messages 44
 - status overview 45
 - systems management 19
 - table view 36
 - tables
 - collapsing resources 39
 - expanding resources 39
 - filtering 40
 - selecting rows 39
 - tasks index 34
 - topology view 41
 - tree menu 41
 - user-defined groups 28
 - work pane 35
- two-way chat 88

U

- unacceptable status 55
- undefine z/VM virtual machines for management task 200
- undefined
 - CPCs 28, 64
 - director/timer consoles 29, 65
 - fiber savers 29, 65
- unmanaged resources 28
- USB flash memory drive 10
- user authentication
 - LDAP 4
- user IDs
 - default 203
- user IDs and passwords, default 12
- user interface styles
 - changing 4
 - classic 2, 47
 - enabling users 3
 - tree 2, 15
- user patterns task 123
- user profiles task 123, 124, 129, 203
- user roles 12
- user settings task 126
- user templates task 129
- user-defined groups 28, 66
- users and tasks task 130
- using
 - a remote hardware management console 216
 - online help 80
 - the add object definition task to define undefined director/timer consoles
 - the director/timer console manual definition template to define undefined director/timer consoles 181
 - the fiber saver manual definition template to define undefined fiber savers 29, 65

V

- view activation profiles task 180
- view console event task 130
- view console information task 131

- view console service history task 132
- view console tasks performed 132
- view frame layout task 187
- view licenses task 132
- view only tasks 102
 - configure channel path on/off 174
 - customize/delete activation profiles 174
 - hardware messages 77
 - operating system messages 78
 - OSA advanced facilities 178
- view PVM records task 133, 156
- view security logs task 134
- view service history task 157
- view the VMRM measurement data task 200
- view this guide
 - html version xiv
 - pdf version xiv
- views and work area
 - active tasks 72
 - books 79
 - console actions 73, 81
 - exceptions 70
 - groups 59
 - task list 76

W

- web address format 218
- web browser 215
 - configuring for on the hardware management console 219
 - getting ready to use 219
 - introduction 217
 - remote operation 93
 - remote restart 93
 - requirements 218
- what's new task 134
- work pane 15, 35
- work pane tabs
 - topology 41

Z

- z/VM virtual machine management tasks 194
 - activate 194
 - choose z/VM virtual machines to manage 195
 - deactivate 195
 - edit the VMRM active configuration file 196
 - grouping 196
 - maintain z/VM profiles 198
 - maintain z/VM prototypes 198
 - maintain z/VM virtual machines 199
 - maintain z/VM volume space 200
 - undefine z/VM virtual machines for management 200
 - view the VMRM measurement data 200
 - z/VM virtual network information 201
- z/VM virtual network information task 201

Level 01a

zBX

options

CPC details 52

customize remote service task 100

remote service task 170

transmit service data 156



Printed in USA

SC28-6905-01

