IBM Z

Hardware Management Console Security

Level 02b

SC28-6987-02

Note:

Before you use this information and the product it supports, read the information in "Safety" on page ix, Appendix B, "Notices," on page 41, and IBM Systems Environmental Notices and User Guide, Z125–5823.

Edition notice

This edition, SC28-6987-02b, applies to the IBM Z and IBM LinuxONE servers. This edition replaces SC28-6987-02a.

There might be a newer version of this document in a **PDF** file available on **Resource Link**.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.

Contents

Figures

Tables

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 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 IBM Z® (Z) and IBM LinuxONE™ (LinuxONE) models can use I/O cards such as FICON®, Open Systems Adapter (OSA), InterSystem Channel-3 (ISC-3), RoCE Express, Integrated Coupling Adapter (ICA SR), zHyperLink Express, or other I/O features which are fiber optic based and utilize lasers (short wavelength or long wavelength lasers).

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.

Laser Notice: U.S. FDA CDRH NOTICE if low power lasers are utilized, integrated, or offered with end product systems as applicable. Complies with 21 CFR 1040.10 and 1040.11 except for conformance with IEC 60825-1 Ed. 3., as described in Laser Notice No. 56, dated May 8, 2019.

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

Security is of ever increasing concern as technology advances at an amazing rate. With identity theft hitting millions of Americans each year encompassing credit card fraud, medical information theft, tax return theft, and much more, it is of utmost importance to protect data from unwanted access. The Hardware Management Console (HMC) is designed with such security in mind - controlling users, auditing access, and preventing unintentional access to its managed systems.

This guide provides high-level information on the HMC responsibilities, physical and network security, as well as best practices for keeping your HMC and systems data secure.

Note: References to IBM Z are also applicable to IBM LinuxONE.

Intended audience

This publication is designed for system administrators who configure the Hardware Management Console for managing systems. There is also a chapter for executives that gives a summary of HMC functions and security concepts.

Prerequisite and related information

Before reading this publication, be familiar with the IBM® products. The IBM product publications are available in Resource Link® (https://www.ibm.com/servers/resourcelink).

Hardware Management Console (HMC) and Support Element (SE) information can be found on the console help system.

How to use this publication

This publication can be viewed from Resource Link (https://www.ibm.com/servers/resourcelink), or as a downloadable pdf.

- Chapter 1, “Introduction,” on page 1 and Chapter 2, “What is the HMC?,” on page 3 give an overview of the HMC security.
- Chapter 3, “Secure access to the HMC,” on page 5 and Chapter 4, “Roles of the HMC,” on page 13 provide more details on physical and network security of the HMC and operational control of the HMC.
- Chapter 5, “Logging and audit trails,” on page 33 covers the security logging and audit reports.
- Chapter 6, “Best practices,” on page 35 indicates the best practices for providing security for the HMC.
- Chapter 7, “Executive summary,” on page 37 provides an overview of the HMC security for company executives.
- Finally, an appendix, Appendix A, “HMC versions,” on page 39, lists the various versions of the HMC and their corresponding machine types.

Accessibility

Accessible publications for this product are offered in EPUB format and can be downloaded from Resource Link at http://www.ibm.com/servers/resourcelink.

If you experience any difficulty with the accessibility of any IBM Z® and IBM LinuxONE information, go to Resource Link at http://www.ibm.com/servers/resourcelink and click **Feedback** from the navigation bar on the left. In the **Comments** input area, state your question or comment, the publication title and

number, choose **General comment** as the category and click **Submit**. You can also send an email to reslink@us.ibm.com providing the same information.

When you send information to IBM®, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Accessibility features

The following list includes the major accessibility features in IBM Z and IBM LinuxONE documentation, and on the Hardware Management Console and Support Element console:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Customizable display attributes such as color, contrast, and font size
- Communication of information independent of color
- Interfaces commonly used by screen magnifiers
- Interfaces that are free of flashing lights that could induce seizures due to photo-sensitivity.

Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

Consult assistive technologies

Assistive technology products such as screen readers function with our publications, the Hardware Management Console, and the Support Element console. Consult the product information for the specific assistive technology product that is used to access the EPUB format publication or console.

IBM and accessibility

See http://www.ibm.com/able for more information about the commitment that IBM has to accessibility.

Revisions

Within each topic, a technical change from the previous edition of the information is indicated by double angle brackets ( ) surrounding the text or illustration.

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).

Summary of changes

Summary of changes for SC28-6987-02b

This update contains the following new technical changes:

- Support for the new default password rule for California Senate Bill No. 327.

Summary of changes for SC28-6987-02a

This update contains the following new technical changes:

- Support for the RSA SecurID tokens through the IBM Multi-Factor Authentication for z/OS product was added.

Summary of changes for SC28-6987-02

This update contains the following new technical changes:

- New TCP/IP inbound and outbound source ports for the no-DVD updates. See Table 1 on page 6 and Table 2 on page 7.
- New STORAGEADMIN system default user added to Table 3 on page 15.
- System default ensemble-related managed resource roles and z/VM® virtual machine tasks are not supported on IBM z15™.
- Table 11 on page 39 updated to include z15™.

Chapter 1. Introduction

The Hardware Management Console (HMC) manages and controls your IBM Z®, zEnterprise® Systems, System z10®, System z9®, zSeries, and S/390® processors. It provides a graphical user interface, single point of control and single-system image for these hardware elements and other associated devices. In addition to providing the access point for users, the HMC also provides a single point of control for automation and provides automation interfaces that use industry-standard protocols.

The servers and operating systems that run on them are significant investments. Therefore, it is critical for the HMC to manage these resources in the most secure manner possible. The purpose of this document is to outline the features of the HMC that relate to security, so that the HMC can be used in a manner that meets each customer's security needs.

Chapter 2. What is the HMC?

Before the specific responsibilities of the HMC and their security implications are discussed, it is important to understand exactly what the HMC is and is not.

- The HMC is an orderable feature of an IBM Z. At least one HMC is required for all the capabilities of an IBM Z to be fully operational. The HMC feature consists of a standard PC hardware platform, which includes a keyboard, mouse, and display, along with preinstalled Licensed Internal Code that provides its various functions. Starting in HMC version 2.13.0, there is a 1U server option for including the HMC and display in the rack.
- The HMC is a closed platform. Specifically, closed means that the customer is not given access to the underlying operating platform and is not allowed to install and run other applications on the HMC. All configuration of the HMC is done by using tasks that are provided by the HMC Licensed Internal Code.
- The HMC is intended and required to be a network-attached device because the HMC uses the network to communicate with various system resources. The HMC Licensed Internal Code application provides the controls to configure the network for the HMC's use. The customer is expected to use normal procedures, such as periodic network scans, to test the HMC for network security.
- The HMC hardware is not serviced by the customer; service representative is responsible for this task.
- The HMC is not an operating platform that is directly usable by the customer; the HMC Licensed Internal Code, which provides the HMC application, is the only feature of the HMC that the customer is entitled to use.

In short, the HMC is considered an appliance whose purpose is to provide management and control of Z mainframes and their associated operating systems and devices.

Chapter 3. Secure access to the HMC

The HMC provides a complete set of controls for the customer to manage user access and capabilities. None of this security matters if the HMC is left logged on in a nonsecure location or if the HMC can easily be attacked through the network. For these reasons, both physical security and network security are critical to the security of the HMC.

Physical security

The physical location of the HMC can play a large role in how the HMC is treated from a security perspective. Often the HMC is in a secure room, which provides the best security. However, securing physical access to the HMC does not negate the need to use the other security features of the HMC, such as automatically disconnecting inactive users and employing strict password rules.

In addition to the security features that the HMC Licensed Internal Code application provides, the PC platform of the HMC also provides some features that can provide extra physical protection to prevent the PC from being initialized with code other than what is installed on the PC hard disk drive. You can use the following functions, which are provided as part of the BIOS (basic input/output system) on the PC:

- Change the startup device settings to prevent starting from removable media, such as a CD or DVD. In version 2.13.0 or higher, boot from removable media is disabled by default on HMCs and SEs.

  Note: If this level of security is active, you need to enable this setting for several processes service personnel perform infrequently, such as hard disk restoration and EC upgrades.
- Set a power-on password to prevent unauthorized changes to BIOS settings.
- Set unattended start mode to allow the HMC to start without the power-on password when power is restored from an unplanned outage.
- Set an admin password for uEFI(Unified Extensible Firmware Interface)/BIOS settings.

  Note: If this level of security is active, the SSR needs customer input for service actions where boot from media needs to be enabled.

Network security

To be useful, the HMC must be attached to a network, so that it can manage the system resources that are associated with it. In some cases, for HMCs located close to the systems it is managing, this network is a *dedicated* network that is fully contained on a single raised floor. However, when a customer has multiple data centers or attaches the HMC to its corporate intranet to allow for remote access, network security is of utmost importance.

Because the HMC can be a multihomed computer (that is, it has multiple network interfaces), it can be connected to a dedicated network that contains the system resources and the corporate intranet at the same time. In fact, this configuration is a prevalent customer configuration because it provides a level of physical separation for the system resources, while simultaneously allowing for the use of advanced HMC capabilities, such as remote access and Internet connectivity for remote support.

The HMC Licensed Internal Code includes a full-function firewall that controls network access to the HMC. By default, the HMC allows almost no inbound network traffic. HMC to SE communications ports are opened as System and zBX Nodes are defined to the HMC. Also, as different features of the HMC are enabled (for example: remote access, SNMP-based automation, Web Services automation), more inbound network traffic is allowed. The following table shows the various TCP/IP ports that the HMC uses for inbound network traffic.

Note: There is no ability for the customer to control the internal firewall, other than through enabling and disabling HMC/SE features.

Table 1. Hardware Management Console inbound traffic from customer networks	
TCP/IP Source Port	**Usage**
TCP 57, 69, 4011 UDP 67, 68, 69, 4011	**Manage Console Recovery** task. These ports utilized for allowing the HMC to become a Boot Server for a selected Recovery Image when the Boot Server is successfully started on the **Manage Console Recovery** task.
ICMP Type 8	Establish communications with system resources that are managed by the Hardware Management Console.
TCP 58787 - 58788 UDP 58788	Automatic discovery of Z mainframes
TCP 4455	Automatic discovery of Director/Timer consoles. **Note:** This is not supported in HMC version 2.13.0 or higher.
UDP 9900	Hardware Management Console to Hardware Management Console automatic discovery.
TCP 55555	SSL encrypted communications from Z mainframes. The internal firewall allows inbound traffic only from the Z mainframes that are defined to the Hardware Management Console.
TCP 9920	SSL encrypted communications from Hardware Management Consoles and Z mainframes.
TCP 443	Remote user access to the Hardware Management Console. Inbound traffic for this port is only allowed by the internal firewall if **Remote operation** is **Enabled** for the Hardware Management Console by using the **Customize Console Services** task.
TCP 9950 - 9959	Proxy **Single Object Operations** sessions to a Z mainframe.
TCP 9960	Remote user applet-based tasks. Inbound traffic for this port is only allowed by the internal firewall if **Remote operation** is **Enabled** for the Hardware Management Console by using the **Customize Console Services** task.
UDP 161 TCP 161 TCP 3161	SNMP automation of the Hardware Management Console. Inbound traffic for these ports is only allowed by the internal firewall when SNMP automation is enabled by using the **Customize API Settings** task.
TCP 5988 TCP 5989 UDP 427	CIM automation of the Hardware Management Console. Inbound traffic for these ports is only allowed by the internal firewall when CIM automation is enabled by using the **Customize API Settings** task.
TCP 6794	Web Services SSL encrypted automation traffic. Inbound traffic for this port is only allowed by the internal firewall when Web Services automation is enabled by using the **Customize API Settings** task.
TCP 61612	Connecting to the Web Services API message broker and flowing Streaming Text Oriented Messaging Protocol (STOMP) over the connection when the Web Services API is enabled by using the **Customize API Settings** task.
TCP 61617	Connecting to the Web Services API message broker and flowing OpenWire over the connection when the Web Services API is enabled by using the **Customize API Settings** task.
UDP 123	Set the time of the Z mainframes.
UDP 520	Interactions with routers and only used on the Hardware Management Console if **routed** is enabled on the Routing tab of the **Customize Network Settings** task.

Table 1. Hardware Management Console inbound traffic from customer networks (continued)	
TCP/IP Source Port	**Usage**
TCP 22	Remote access by Product Engineering and only allowed by the internal firewall if remote product engineering access is configured by using the **Customize Product Engineering Access** task. Also, on an alternate HMC within an ensemble, allows the primary HMC to establish a connection with the alternate HMC for replicating configuration information.
TCP 21	Inbound FTP requests. This port is only enabled when Electronic Service Agent or the **Enable FTP Access to Mass Storage Media** task is being used. FTP is an unencrypted protocol; for maximum security these tasks must not be used on the Hardware Management Console.
TCP 3900 - 3909	Running the Remote Control Applet of the Advanced Management Module (AMM) within a z BladeCenter Extension (zBX).

In addition to these inbound requests, the HMC also initiates requests to the system resources that it is managing, and to other HMCs. The following table shows the types of outbound network traffic that is initiated by the HMC.

Table 2. Hardware Management Console outbound traffic to customer networks	
TCP/IP Source Port	**Usage**
TCP 57, 69, 4011 UDP 67, 68, 69, 4011	**Manage Console Recovery** task. These ports utilized for allowing the HMC to become a Boot Server for a selected Recovery Image when the Boot Server is successfully started on the **Manage Console Recovery** task.
ICMP Type 8	Establish communications with system resources that are managed by the Hardware Management Console.
UDP 9900	HMC-to-HMC automatic discovery.
TCP 58787 UDP 58787	Automatic discovery of and establishing communications with Z mainframes.
TCP 55555	SSL encrypted communications to Z mainframes. The internal firewall allows only inbound traffic from the Z mainframes that are defined to the HMC.
TCP 9920	SSL encrypted communications to Hardware Management Consoles and Z mainframes.
TCP 443	**Single Object Operations** to a Z mainframe console.
TCP 9960	Applet-based tasks during a **Single Object Operations** session for a Z mainframe console.
TCP 25345	**Single Object Operations** to a Z mainframe console.
TCP 4455	Communications with Director/Timer consoles being managed by the Hardware Management Console. **Note:** This is not supported in HMC version 2.13.0 or higher.
UDP 161	Communications with IBM Fiber Saver managed by the Hardware Management Console. **Note:** This is not supported in HMC version 2.13.0 or higher.
TCP x	User authentication that uses an LDAP server where *x* is the port that the LDAP server is running on.
TCP 443	Call-home requests as part of the Remote Support Facility (RSF).

Table 2. Hardware Management Console outbound traffic to customer networks (continued)	
TCP/IP Source Port	**Usage**
TCP 3900	Running the Remote Control Applet of the Advanced Management Module (AMM) within a z BladeCenter Extension (zBX).
TCP 21	Load system software or utility programs.
TCP 22	Retrieve the SSH public key of hosts, by using the **Manage SSH Keys** task, for securing SSH File Transfer Protocol (SFTP) connections to FTP servers. Also, used for the SFTP connections. In addition, on a primary HMC within an ensemble, allows the primary HMC to establish a connection with the alternate HMC for replicating configuration information.
UDP 123	Connecting to a Network Time Protocol (NTP) server.
TCP 25	Send email events to a Simple Mail Transfer Protocol (SMTP) server for delivery, by using the **Monitor System Events** task, when the HMC is configured. (Might be a port other than 25, but 25 the default SMTP port that most SMTP servers use.)

SSLv3 and RC4 compatibility

Secure Sockets Layer (SSL) version 3 and Rivest Cipher 4 (RC4) protocols are used in popular Internet protocols such as Transport Layer Security (TLS). The HMC and SE might negotiate these protocols for specific secure communications (that is, if one side indicates that is the only communication method it can use). However, since it is possible to attack SSL/TLS connections that use RC4 as the block cipher algorithm, it is recommended to disable SSLv3 and RC4 where possible. Microcode Levels (MCLs) are available at all HMC/SE versions that provide more secure, state of the art cipher suites, as well as the ability to manage SSLv3 and RC4 compatibility.

Use the **Customize Console Services** task, **SSLv3 and RC4 compatibility** service, to control whether the HMC supports the SSLv3 protocol and RC4 cipher when the console establishes specific secure connections. Disabling this service ensures that the HMC does not negotiate SSLv3 protocol and RC4 cipher. See the online help for the **Customize Console Services** task to see which secure connections might use SSLv3 and RC4.

Disabling this service can cause connections to and from HMCs and SEs to be unsuccessful if the HMCs and SEs are at a level that does not include this corresponding service. Thus, unlike other console services, the **SSLv3 and RC4 compatibility** service is enabled by default to allow compatibility with prior HMC/SE versions that do not have the current MCLs applied. The recommendation is to first apply the current MCLs to all HMCs and SEs, then use **Customize Console Services** to disable the **SSLv3 and RC4 compatibility** service on all HMCs and SEs.

Malware

The HMC provides a couple mechanisms for protection against Malware getting onto the HMC or SEs. IBM provides protection of all HMC/SE Licensed Internal Code (LIC) updates, referred to also as firmware updates, by using digitally signed Firmware (FW). To complement that security, the customer should use Secure FTP for all customer initiated file transfers.

Digitally signed firmware

As previously stated, the HMC provides protection of all firmware updates by using digitally signed firmware. The HMC base code is signed with a private key, including disk image files and individual firmware modules. Firmware fixes (Microcode Fixes (MCFs) packaged into Microcode Levels (MCLs) packaged into Bundles) are signed with a private key and validated during the retrieval process.

Backup Critical Data and the hard disk restore performed by the service representative also use digitally signed firmware. A symmetric key is used during backups to allow validation during the hard disk restore.

The HMC is also in compliance with Federal Information Processing Standard (FIPS) 140-2 Level 1 for the crypto LIC changes.

Firmware tamper detection

Beginning on Version 2.14.0, an enhancement on the Support Element provides notification if tampering with booting of firmware on the CPC is detected. This enhancement is designed to meet the BIOS Protection Guidelines recommended and published by the National Institute of Standards and Technology (NIST) in Special Publication 800-147B. If tampering is detected, the Support Element issues a customer alert with a warning or a lock of the Support Element, depending on the configuration. If call home support is enabled on the Hardware Management Console managing the Support Element, additional analysis of the Support Element is performed and displayed by IBM Resource Link.

In addition to this support, the Hardware Management Console also has been enhanced to provide attempted tamper monitoring and reporting. A newly manufactured Hardware Management Console directly ordered with the system, or at a later time, is required for this protection. Any detected event of attempted tampering is logged and is issued a customer alert with a warning or a lock of the Hardware Management Console, depending on setup configuration. If call home support is enabled on the Hardware Management Console, supplementary analysis of events logged by the Hardware Management Console are available on the IBM Resource Link

Although you can carry forward your Hardware Management Consoles, these tamper protection capabilities are delivered only on newly manufactured Hardware Management Consoles. The system environment can contain both Hardware Management Consoles that have been carried forward and newly manufactured Hardware Management Consoles.

Secure FTP (SFTP)

Beginning on version 2.11.1, the HMC supports usage of a secure File Transfer Protocol (FTP) connection from an HMC/SE FTP client to a customer FTP server location.

This support is implemented by using the SSH File Transfer Protocol; an extension of the Secure Shell (SSH) protocol. SSH is a cryptographic (encrypted) network protocol for initiating text-based shell sessions on remote servers in a secure way. The **Manage SSH Keys** task is used to associate a public key with a host address. Secure FTP infrastructure allows HMC/SE applications to query if a public key is associated with a host address and then utilize the Secure FTP interface with the appropriate public key for that host.

FTPS

Beginning on version 2.14.0, the HMC now supports secure File Transfer Protocol (FTP) operations using the FTPS (FTP with SSL) protocol. To allow a secure connection to an FTPS server, the server's certificate must be imported to the HMC using the **Certificate Management** task. With the addition of FTPS support, the HMC tasks now support three FTP protocols: plain FTP, FTPS (FTP with SSL), and SFTP (SSH based FTP).

The following tasks now have options to use any of the three supported protocols:

- **Advanced Facilities (SE) / OSA Advanced Facilities (HMC) → Export Adapter Diagnostics Data**
- **Advanced Facilities (SE) / OSA Advanced Facilities (HMC) → Manage Security Certificates → Export/ Import Certificates via FTP**
- **Advanced Facilities (SE) / OSA Advanced Facilities (HMC) → View Port Parameters → Export via FTP**
- **Archive Security Logs → Archive to FTP server**
- **Analyze Console Internal Code → Retrieve MFC from FTP server**
- **Change Console Internal Code → Retrieve internal code changes → Retrieve code changes from FTP site to the Hardware Management Console**
- **Configure Backup Settings**
- **Cryptographic Configuration → UDX Configuration → Import from FTP Server**
- **Customize Scheduled Operations → Audit and Log Management**

- **FCP Configuration → Export or Import Configuration → FTP site**
- **Input/Output (I/O) Configuration → Import/Export Source File → FTP Location**
- **Load from Removable Media or Server**
- **OSA Advanced Facilities → Card Specific Advanced Facilities → Manual Configuration Options → Import/Export source file by FTP** (OSC channel type)
- **Retrieve Internal Code → Retrieve Internal Code Changes**
- **Save Upgrade Data→ FTP server**
- **System Input/Output (I/O) Configuration Analyzer → Import/Export Source File → FTP Location**
- **View Security Logs → Retrieve from FTP server**

Proxy FTP

Beginning on version 2.14.0, the SE no longer connects directly to customer FTP servers; instead the HMC acts as an FTP proxy for Support Element tasks performing FTP operations. This makes it easier to maintain an isolated network for the Z mainframe as described in the Chapter 6, “Best practices,” on page 35 section. As a result, any SE that attempts to perform an FTP operation must be defined to at least one HMC with connectivity to the target server. Also, the HMC must have imported the target server's security certificate or SSH key when using FTPS or SFTP respectively.

Communications

From a network perspective, the HMC uses TCP/IP for all of its communications. The HMC fully supports both IPv4 and IPv6. When using the previous information to define rules in customer-owned firewall roles, the customer might need to define rules for each of these protocols. Additionally, even though the HMC is a management focal point for various system resources, the HMC does not provide any IP forwarding capabilities.

The management of the various system resources requires network communications between the HMC and the resources. It is important for this communication to be secure. There are different types of network communications for each of the Z mainframes and system resources.

Z mainframes

All network communications between the HMC and the Z mainframes are AES encrypted except the communications for automatic discovery and the initial communication establishment. Ephemeral keys for this encryption are negotiated using the Secure Remote Password (SRP) protocol. The Domain Security password, along with a private key stored in the HMC Licensed Internal Code are used in the key negotiation protocol. It is recommended that a custom Domain Security password be used if possible. In addition to being encrypted, the data send to and from the Z mainframe is obfuscated to make it more difficult to replicate.

Director/Timer consoles

Communications with a Sysplex Timer or ESCON Directory console fall into two categories. The first type is for discovery and query of console information. Because this communication is a query-only type of communication, there is no need to encrypt this network traffic. The second type of communication provides remote access to the screen of the Director/Timer consoles by using VNC-like communications. This flow of data is also not encrypted.

Note: Director/Timer console is available in HMC Version 2.12.1 and prior.

IBM Fiber Savers

The main role the HMC plays regarding IBM Fiber Savers is to provide call-home support for these devices. All of the data that the HMC knows about these devices is obtained by using the standard SNMP

support that is provided in the devices. This SNMP communication is a read-only type of flow and is not encrypted.

Note: IBM Fiber Savers are available in HMC Version 2.12.1 and prior.

Chapter 4. Roles of the HMC

The HMC plays many different roles in the management of system resources. There are security aspects for almost all of these roles. The major roles of the HMC are as follows:

- User operational control
- Automated operational control
- Service and support.

Each of these roles has security implications that customers must consider to ensure that the HMC adheres to their security requirements. Before you discuss the security aspects of each of these roles, it would be worthwhile to mention one of the HMC's security tenets: Any configurable feature of the HMC that might raise security concerns is always disabled by default. This approach forces the system administrator to think about each of these features when explicitly enabling them.

Note: When the HMC is upgraded from one version to another, the previous configurable settings are saved and restored. Thus, in the case of an upgrade, all configurable features that safeguard security are not disabled by default; the settings are retained from the previous version.

User operational control

One of the primary roles of the HMC is to provide a web-based graphical user interface for managing and controlling various system resources. The main user interface allows the user to perform various tasks, some of which affect the HMC itself, while others target system resources. This user interface provides access to all of the features of the HMC Licensed Internal Code application. Additionally, this user interface is the only access that is provided for customer use.

Remote user access

At first glance, it is fairly obvious that the web-based user interface provided locally on the HMC is rendered by using a browser. This design point makes it technically straightforward to provide the same user interface to a remote browser through the network. However, there are security aspects to consider regarding remote access.

Accessing the web-based graphical user interface of the HMC from a remote browser requires setting the **Customize Console Services** task to enable remote operation. Enabling remote user access allows the HMC to accept incoming requests. The implication here is that, by default, the HMC blocks all incoming Hypertext Transfer Protocol (HTTP) requests at the network level. In addition, it is important to understand that enabling this feature results in the HMC's accepting only Secure Sockets Layer (SSL) based HTTP requests. More specifically, the HMC never accepts remote, nonsecure HTTP requests.

When the HMC is enabled for remote operation, specific users can then be enabled to allow remote access. The access administrator can set this ability by using the **User Management** task (or the **User Profiles** task in HMC version 2.12.1 or earlier) and setting the **Allow remote access to the console** check box.

Web server certificates

As previously described, all remote user access to the HMC uses SSL-encrypted connections. While the encryption of the data that flows over the network is important, in some cases it is equally important to use certificates to control some of the parameters for the encryption on these connections.

When first started, the HMC creates a self-signed certificate that can be used for encrypting data for remote user connections. In many cases, the self-signed certificate is sufficient for the customer, and the system administrator needs to do nothing further. However, if a self-signed certificate is not sufficient, the system administrator needs to use the **Certificate Management** task to create a certificate that meets the needs of the customer. This task provides a full complement of certificate-related functions;

from creating a self-signed certificate to providing all the tools needed to allow usage of a certificate signed by one of today's many certificate authorities.

It is worth noting that if the self-signed certificate that the HMC generates is not replaced, there is a risk of a "man-in-the-middle" attack. To create more secure connections, use the **Certificate Management** task to create a certificate that is not self-signed but instead signed by a certificate authority.

In addition to creating a certificate to provide for more security for remote user access, the **Certificate Management** task can also be used to control the cipher suites that are used when each SSL-encrypted connection is made to the HMC.

Again, the important point to understand is that all remote user access is performed by using SSL-encrypted communications. The HMC provides a full complement of capabilities to allow the customer to customize the certificates and cipher suites that are used for the encryption. Use the **Configure SSL Cipher Suites** advanced option of the **Certificate Management** task to specify which SSL cipher suites are allowed to be used for SSL connections to this console. The SSL connections for which these cipher suites apply are those connections from remote web browsers or from web services API programs that connect to the HMC API HTTP server.

User Management task

Beginning with version 2.13.0, the **User Management** task provides a convenient dashboard to manage all aspects of system users that log on to the HMC. This task replaces the following tasks in support of user operational control:

- **User Profiles**
- **Customize User Controls**
- **User ID Patterns**
- **User Templates**
- **Password Profiles**
- **Manage Enterprise Directory Server Definitions**

The **User Management** task gives the access administrator a common area to view and manage users, roles, user patterns, user templates, password rules, and LDAP server definitions for your system. The navigation icons on the dashboard are listed in the order of highest usage and not the sequence an administrator would use to initially set up access to the console. The task **Help** *Getting Started* section has some scenarios to assist an administrator with first-time usage of the **User Management** dashboard. Also, the *Default Permissions* section of the help contains the list of permissions that are granted to every user by default and therefore not shown on the **User Management** dashboard.

The **User Management** navigation icons on the dashboard correspond to the tasks necessary for user operational control. There is a **New** wizard for each of the navigation icons that provides a guided step-by-step process for each new definition. The wizard supports creation of a new definition from scratch or based on an existing definition.

Users
A *user* object defines the user's authentication, roles that determine access permissions, and settings that control remote access, Web Services access, and various sessions timeouts.

Roles
A *role* defines permission to tasks, types of objects or specific objects, groups, and task lists.

User Patterns
A *user pattern* is used to automatically create users on the system based on successful authentication of user IDs that conform to a defined string pattern.

User Templates
A *user template* defines the settings and permissions for users who are authenticated with a user pattern. The template requires an LDAP server definition.

Password Rules
A *password rule* defines a set of rules to be used when users or administrators are creating a user password.

LDAP Server Definitions
An *LDAP server definition* specifies host connection and directory entry location information to be used for authentication.

Multi-factor Authentication
A *multi-factor authentication* is used to provide for the identification of users by means of the combination of multiple, different components.

The next sections cover these functions in more detail.

Users

Before the user interface or tasks can be accessed, either remotely or locally, the HMC must first authenticate a user. Authentication is accomplished by logging on the HMC with a user ID and password. Multiple users can access the HMC at the same time. Also, a single user can have multiple logon sessions active at the same time. Each user has unique saved sessions on disconnect.

A *user* object defines the user name (user ID), the user's authentication, and roles that determine access permission. By default, the HMC includes a set of eight default users (ENSADMIN and ENSOPERATOR are added in HMC version 2.11.0). These eight system defined users align with a set of traditional user classifications for the HMC. The default user IDs and their classifications are as follows:

Table 3. System default users

User ID	**Classification**
ACSADMIN	Access administrator
ADVANCED	Advanced operator
OPERATOR	Basic operator
SERVICE	Service representative
STORAGEADMIN	Storage administrator
SYSPROG	System programmer
ENSOPERATOR (2.14.1 and lower)	Ensemble operator
ENSADMIN (2.14.1 and lower)	Ensemble administrator

These default users are provided to illustrate how different users allow for the operational control of the system resources by operations, administrative, and service representatives with various levels of expertise and needs. You cannot modify which roles are assigned to the system defined default users, nor can you modify the system default roles. You can make your own copies based on the system defaults.

For the HMC to be secure, you must remove these default user IDs from the HMC, disable the user IDs, or at a minimum, change their passwords. Before you remove the default users, copy the user definition and modify it according to your company requirements.

In addition, for auditing purposes, it is important that all HMC users have their own user IDs. In other words, to provide a more secure HMC, user IDs for the HMC must not be shared among multiple people.

Creation of custom users and roles provides the benefit of making specific access to required objects and tasks. Custom users also provide the benefit of more granularity in the audit logs; you know exactly who performed specific actions. The system administrator can use the **User Management** task (or the **User Profiles** task in HMC version 2.12.1 or earlier) to manage the users for the HMC. In addition to providing the expected functions of adding, removing, and altering users, this task also controls various aspects of the user. The user definition is specified through the following settings:

- The authentication method for the user: Local or Lightweight Directory Access Protocol (LDAP)
- The password rule for a local authentication user
- The password for a local authentication user
- The LDAP server for an LDAP authentication user
- The roles that are associated with the user; define permission to tasks, type of objects or specific objects, groups, and task lists
- The ability to temporarily disable a user
- The ability to force a password to be changed at the next login
- A users ability to remotely access the HMC
- A users ability to access the Web Services management interfaces
- The number of incorrect login attempts allowed before temporarily disabling the user ID and the amount of time the user ID is disabled
- Whether a user is disabled due to lack of activity (for example, not used for login) and the amount of time that triggers this consequence
- Various timeouts for the user, such as:
  - The minimal time between password changes
  - The time period before the user is automatically disconnected due to inactivity
  - The time period before the user is forced to verify the login session by specifying the correct password
  - The time period before the user is automatically disconnected due to the correct password not being used for verification.

Many settings can be adjusted for users, but this granularity is important because user authentication is one of the most important aspects of security for the HMC. Beginning with version 2.15.0, the HMC users can be used to log on to the Support Element (SE) managed by that HMC.

Passwords

Keeping passwords nontrivial is an important aspect of the security for any computer system. The use of trivial passwords can easily undermine all of the other security features. The evidence of this security requirement can be seen in the many different rules for various passwords all computer users must follow these days. Since no single set of rules works for all customers, the HMC allows the definition and enforcement of user-defined customized password rules.

A *password rule* defines a set of rules to be used when the system administrator or user is creating a user password. As shipped, the HMC provides three default password rules. These default password rules cannot be modified, but they can be removed if they are not associated with any users.

Table 4. System defined default password rules

Rule name	Description
Basic	Simple rule that defines a minimum length of 4 and a maximum length of 8 and allows for alphabetic and numeric characters. This rule is provided mainly to permit continued use of the traditional passwords of the default user IDs. **Note:** Basic is the default rule for newly created user IDs in HMC version 2.12.1 or lower. For a more secure HMC, you must modify new user IDs to use a rule that meets security requirements for the company.
Strict	Defines a minimum length of 6 and a maximum length of 8, allows alphabetic and numeric characters, and requires the password to start and end with an alphabetic character. The rule also prevents the password from having the same character more than twice in a row and causes the password to expire in 180 days.

Table 4. System defined default password rules (continued)	
Rule name	**Description**
Standard	Defines a minimum length of 6 and a maximum length of 30 and allows for alphabetic, numeric, and special characters. The password must start and end with an alphabetic or special character and must have at least one alphabetic character in between. The rule also prevents the password from having the same character more than twice in a row and causes the password to expire in 186 days. In addition, the password cannot be the same as one of the last four passwords for the user and cannot be similar in more than 3 characters with the last password for the user. **Note:** Standard is the default rule for newly created users in HMC version 2.13.0 or higher.

Each customer is expected to review the default set of password rules relative to the policies defined for the company. The system administrator can then create new password rules so that they adhere to the company's policy. The system administrator can use the **User Management** task (or the **Password Profiles** task in HMC version 2.12.1 or earlier) to manage the password rules for the HMC. This task defines the following set of characteristics for password rules:

- Minimum length
- Maximum length
- Number of days before the password expires
- Maximum number of times a character can be used consecutively within a password
- Number of times a password must be changed before a previous password can be reused
- Whether the characters in the password are case-sensitive
- Specific rules about the types of characters that can be used in a password and in which positions.

Since the introduction of the California Senate Bill No. 327 starting January 1, 2020, the usage of default passwords are now banned. This affects machines that are shipped to California, so all default passwords on the system are reset before they are shipped and require that passwords be updated the first time that they are used to log on. Additionally, new functionality has been added to the **User Management** task that provides this support. The only users that have access to this functionality are Product Engineering, a user with permission to the **User Management** task and SERVICE. However, SERVICE has limited scope when using this new functionality.

Multi-factor authentication

Beginning with z14, support for multi-factor authentication (MFA) was added. This added an optional second authentication factor in addition to a user's console login password when accessing the console. Specifically, the user must enter a 6-digit authentication code a Time-based One-Time Password (TOTP) as defined by RFC 6238 which is based on the current time and a 32-character user-specific shared secret key. The TOTP is validated by the console with no dependencies for network connectivity or outside components or products. There are many freely available smartphone apps that can be configured with the user's shared secret key to generate the user's current TOTP.

Beginning with z15, support for the RSA SecurID tokens through the IBM Multi-Factor Authentication for z/OS product was added. When a user is required by the system administrator to use RSA SecurID when logging onto the HMC, the user must supply their current RSA SecurID passcode and their HMC user ID and logon password. After validating the HMC user ID and password, the HMC passes the user’s MFA user ID and the supplied RSA SecurID passcode to the IBM MFA instance associated with the HMC user ID. The IBM MFA verifies that the IBM MFA user ID is known to it and is configured to use RSA SecurID. IBM MFA then contacts the customer's RSA SecurID Authentication Manager server to validate the user’s RSA user ID and the passcode supplied by the user.

Enterprise directory server (LDAP)

It is possible to define users that are authenticated by using an Enterprise Directory or LDAP server. The system administrator can use the **User Management** task (or the **Manage Enterprise Directory Server Definitions** task in HMC version 2.12.1 or earlier) to define one or more servers that can authenticate passwords for users.

This method of user authentication makes a great deal of sense for customers who already have a well established LDAP server configuration. When a user is associated with an LDAP server definition, all the rules for defining a password, its expiration, and so forth, are already in place and applied. Because an existing LDAP configuration meets the customer's security needs, the customer does not need to consider these factors when evaluating the security aspects of the HMC.

For more secure operating characteristics, it is recommended that the HMC is configured to use SSL communications with the LDAP server if possible. In fact, for the most secure LDAP authentication, the LDAP server should use a server-specific certificate that is signed by a trusted certificate authority. If the LDAP server's certificate is not signed by one of the well-known certificate authorities (for example, if it is signed by a corporate signing certificate), the necessary signing certificates must be imported into the HMC by using the **Certificate Management** task and the server definition must be configured not to tolerate self-signed or otherwise untrusted server certificates (the default).

Note: At least one user with administrator capabilities, who is not authenticated by an LDAP server, is required (for example: ACSADMIN). This requirement ensures that HMC can still be used when the network or LDAP server fails, which would prevent authentication for users who are defined to use an LDAP server.

User roles

The HMC provide numerous tasks that can be performed on the HMC itself and on the various system resources that it is managing. Not all tasks are intended for all HMC users. For this reason, the HMC provides an initial set of *roles* that group these tasks and resources into sets that align with a set of traditional HMC user classifications.

Prior to version 2.13.0, there were two types of HMC roles: task roles and managed resource roles. Task roles group tasks into sets that make sense for specific classifications of users. Likewise, managed resource roles group specific types or instances of system resources that specific classes of users are allowed to manage. In version 2.13.0, with the **User Management** task, a single role can contain any combination of tasks, types of objects or specific objects resources, groups, and task lists. Thus, the system administrator can customize a single role for a user or group of users that contains all the permissions necessary.

The HMC ships the following default roles:

Table 5. System default managed resource roles (excluding ensemble-related managed resources roles)

Managed resource role	HMC version	Description
All Directors/Timers Managed Objects	2.12.1 and lower	Allows access to both defined and undefined Director/Timer managed resources.
All Fiber Saver Managed Objects	2.12.1 and lower	Allows access to both defined and undefined Fiber Saver managed resources.
All Resources	2.12.0 and higher	Allows access to all defined and undefined managed objects (includes all objects of all types).
All Managed Objects	2.9.0 through 2.10.2	Allows access to all Defined CPC, Undefined CPC, CPC Image, and Coupling Facility managed resources.

Table 5. System default managed resource roles (excluding ensemble-related managed resources roles) (continued)

Managed resource role	HMC version	Description
All zCPC Managed Objects	2.11.0 through 2.12.1	Allows access to all Defined CPC, Undefined CPC, CPC Image, and Coupling Facility managed resources. **Note:** With the addition of Ensembles, this role was renamed from All Managed Objects
All System Managed Objects	2.13.0 and higher	Allows access to all Defined CPC, Undefined CPC, Defined zBX Nodes, Undefined zBX Nodes, CPC Image, and Coupling Facility managed resources. **Note:** With the addition of zBX Nodes, this role was renamed from All zCPC Managed Objects
Defined Directors/Timers Managed Objects	2.12.1 and lower	Allows access to defined Director/Timer managed resources.
Defined Fiber Saver Managed Objects	2.12.1 and lower	Allows access to defined Fiber Saver managed resources.
Defined zCPC Managed Objects	2.11.0 through 2.12.1	Allows access to all Defined CPC, CPC Image, and Coupling Facility managed resources.
Defined System Managed Objects	2.13.0 and higher	Allows access to all Defined CPC, Defined zBX Nodes, CPC Image, and Coupling Facility managed resources. **Note:** With the addition of zBX Nodes, this role was renamed from Defined zCPC Managed Objects
Limited Managed Objects	2.10.2 and lower	Allows access to all Defined CPC and CPC Image
z/VM Virtual Machine Objects	2.14.1 and lower	Allows access to all defined z/VM virtual machine objects.

Table 6. System default ensemble-related managed resource roles

Managed resource role	HMC version	Description
All Resources	2.12.0 and higher	Allows access to all defined and undefined managed objects (includes all objects of all types).
BladeCenter Objects	2.14.1 and lower	Allows access to blade center objects.
DPXI50z Blade Objects	2.14.1 and lower	Allows access to DataPower® XI50z blade objects.
Ensemble Object	2.14.1 and lower	Allows access to the ensemble object.
IBM Blade Objects	2.14.1 and lower	Allows access to general purpose IBM blade objects.
IBM Blade Virtual Server Objects	2.14.1 and lower	Allows access to blade virtual server objects.

Table 6. System default ensemble-related managed resource roles (continued)		
Managed resource role	**HMC version**	**Description**
Storage Resource Objects	2.11.0 and higher	Allows access to storage resource objects.
Virtual Network Objects	2.14.1 and lower	Allows access to ensemble-related virtual network objects.
Workload Objects	2.11.0 and higher	Allows access to workload objects.

Table 7. System default task roles (excluding ensemble-related task roles)		
Task Role	**HMC version**	**Description**
Access Administrator Director/ Timer Tasks	2.12.1 and lower	Administrative tasks for Director/Timer managed resources.
Access Administrator Fiber Saver Tasks	2.12.1 and lower	Administrative tasks for Fiber Saver managed resources.
Access Administrator Tasks	All	Administrative tasks for the HMC, CPC, CPC Image, and Coupling Facility managed resources.
Advanced Operator Tasks	All	Advanced operational tasks for the HMC, CPC, CPC Image, and Coupling Facility managed resources.
CIM Actions	All	Tasks that are used for automation through CIM.
Operator Tasks	All	Operational tasks for the HMC, CPC, CPC Image, and Coupling Facility managed resources.
Service Fiber Saver Tasks	2.12.1 and lower	Service related tasks for Fiber Saver managed resources.
Service Representative Director/ Timer Tasks	2.12.1 and lower	Service related tasks for Director/Timer managed resources.
Service Representative Tasks	All	Service related tasks for the HMC, CPC, CPC Image, and Coupling Facility managed resources.
System Programmer Tasks	All	System Programmer tasks for the HMC, CPC, CPC Image, and Coupling Facility managed resources.
Universal Director/Timer Tasks	2.12.1 and lower	Director/Timer tasks that are allowed for all users.
Universal Fiber Saver tasks	2.12.1 and lower	Fiber Saver tasks that are allowed for all users.
z/VM Virtual Machine Tasks	2.14.1 and lower	All tasks relating to z/VM virtual machine images.

Table 8. System default ensemble-related task roles		
Task Role	**HMC version**	**Description**
Energy Management Administrator Tasks	2.11.0 and higher	Administrative tasks for managing power related settings for CPC, BladeCenter, and Blade managed resources.
Ensemble Administrator Tasks	2.11.0 and higher	Tasks that are used for creating and managing the ensemble.
Performance Management Administrator Tasks	2.11.0 and higher	Administrative tasks for managing performance policies for the ensemble.
Performance Management Operator Tasks	2.11.0 and higher	Operational tasks for performance policies.
Policy Administrator Tasks	2.14.1 and lower	Administrative tasks for managing performance and availability policies for the ensemble. **Note:** With the addition of Availability Policies, this role was renamed from Performance Management Administrator Tasks.
Policy Operator Tasks	2.14.1 and lower	Operational tasks for performance and availability policies. **Note:** With the addition of Availability Policies, this role was renamed from Performance Management Operator Tasks.
Storage Resource Administrator Tasks	2.11.0 and higher	Administrative tasks for managing storage resources in the ensemble.
Virtual Network Administrator Tasks	2.14.1 and lower	Administrative tasks that are used for managing virtual networking objects in the ensemble.
Virtual Server Administrator Tasks	2.14.1 and lower	Administrative tasks for managing virtual servers in the ensemble.
Virtual Server Operator Tasks	2.14.1 and lower	Operational tasks for virtual server managed resources.
Workload Administrator Tasks	2.11.0 and higher	Administrative tasks for managing workload resources in the ensemble.

The system administrator can use the **User Management** task (or **Customize User Controls** task for HMC version 2.12.1 or earlier) to define new tasks or managed resource roles that make sense in the environment. Likewise, as previously mentioned, the **User Management** task (or the **User Profiles** task for HMC version 2.12.1 or earlier) associates one or more roles with a specific user.

Users templates and user patterns

In addition to defining users that authenticate locally or through an LDAP server, the HMC allows creation of temporary users who authenticate through an LDAP server if their user ID matches a defined user pattern. The permissions for the temporary user are defined in a user template similar to a user definition. Since the user pattern definition requires selection of a user template for authentication, the user template definition must be created first.

User templates

A *user template* defines the settings and permissions for users who are authenticated with a user pattern. The template requires an LDAP server definition. When a user logs on, if the user ID is not defined locally, it is matched against all the user patterns defined. If a match is found, the user ID is then validated against entries in the LDAP server that is specified by the template that is specified in the matching user pattern.

The system administrator can use the **User Management** task (or the **User Templates** task in version 2.12.1 or earlier) to manage the user templates for the HMC. In addition to providing the expected functions of adding, removing, and altering user templates, this task also controls various aspects of the user. As with the user definition, the user template definition is specified through the following settings:

- The LDAP server to use for authentication
- The roles that are associated with the user; define permission to tasks, type of objects or specific objects, groups, and task lists
- The ability to temporarily disable a user template
- A users ability to remotely access the HMC
- A users ability to access the Web Services management interfaces
- The number of incorrect login attempts allowed before temporarily disabling the user template and the amount of time the user ID is disabled
- Whether a user is disabled due to lack of activity (for example, not used for login) and the amount of time that triggers this consequence
- Various timeouts for the user, such as:
  - The time period before the user is automatically disconnected due to inactivity
  - The time period before the user is forced to verify the login session by specifying the correct password
  - The time period before the user is automatically disconnected due to the correct password not being used for verification.

As with users, many settings can be adjusted for user templates.

User patterns

Use the **User Management** task (or the **User Patterns** task for version 2.12.1 or earlier) to define a *user pattern* to be used to try to match "unknown" user IDs with a template. This pattern essentially defines a group of console users whose user IDs all match a certain pattern. These user IDs are validated against entries in your LDAP server. When a user logs on, if the user ID is not defined locally, it is matched against all the patterns defined. The order of the pattern definitions in the list controls the order in which they are tried. When a match is found, a temporary user definition is created from the user template that is named in the pattern definition. The user definition exists only while the user is logged on, though any settings they customize are retained for the amount of retention time that is specified in the pattern definition. If the user logs on again within that period, they do not need to customize the same settings they did previously.

If preferred, you can name an LDAP attribute whose value is the name of the user template that is used for that user instead of the one named in the pattern definition. This capability gives certain users different privileges than the default for that pattern. Additionally, you can name an LDAP attribute whose value is the name of the console domain that is allowed to log on using that LDAP entry. LDAP attributes can have multiple values in an LDAP entry. If this attribute name is specified in the pattern definition, one of the attribute values must match the console's domain name.

Creation of custom temporary users provides the benefit of making specific access to required objects and tasks without having a specific user definition. Temporary users are also logged in the audit and security logs when they are logged on. Thus, you know exactly who performed specific actions, the same as with a specific user definition.

Data replication

The HMC provides many different configuration options for controlling user operation controls, and most customers have multiple HMCs for redundancy. While configuration could be performed separately at each HMC, the data replication feature of the HMC is provided to help in large installations with many HMCs.

For example, the system administrator can use the **Configure Data Replication** task to configure a master HMC that configures all of the user-related characteristics for that HMC and for a set of "slave" HMCs. There is no need to worry about important configuration data being compromised while it is shared with the other HMCs because this data, like all other data sent between HMCs, is encrypted.

Automated operational control

In addition to providing user access, the HMC also can act as a single point of control for automation. The HMC provides automation capabilities by using different industry standard protocols:

- Simple Network Management Protocol (SNMP)
- Common Information Model (CIM)
- Web Services (HTTP).

Again, following the standard theme for access to the HMC, none of these management protocols are enabled by default. The system administrator can use the **Customize API Settings** task to configure access to SNMP, Web Services, and CIM automation.

Note: Prior to version 2.11.0, the **Customize Console Services** task was used to enable CIM automation.

Simple Network Management Protocol (SNMP)

As with enabling remote user access, enabling SNMP automation support through the **Customize API Settings** task allows the HMC to accept incoming SNMP requests that use the standard SNMP ports. The SNMP protocol defines several different authorization schemes for the various SNMP versions that the specifications define. Currently, the only authorization scheme the HMC supports is the SNMP "community based" authorization scheme. The **Customize API Settings** task also allows the system administrator to define these "community names" that are used for authenticating SNMP automation requests. The definition of these communities allows for:

- Controlling the access level that is allowed for a community to be either read-only level or read/write level
- Restricting the use of a community to a set of hosts on the network, based on their network addresses
- Restricting the use of a community to an individual host on the network.

Security is a weakness of SNMP Versions 1 and 2 with authentication limited to just a password (community string) sent in clear text between a manager and agent. SNMP Version 3 provides enhanced security through password-based authentication and encryption. Each SNMPv3 message contains security parameters, which are encoded as an octet string. These security parameters provide the following important security features:

- Confidentiality through the encryption of packets that prevent snooping by an unauthorized source.
- Message integrity that ensures that a packet is not tampered with while in transit. Optionally, a packet replay protection mechanism can be used.
- Authentication by user name and password that verifies that the message is from a valid source.

Specific to the HMC, the **Customize API Settings** task allows the system administrator to define SNMPv3 users that are used for more secure authentication of SNMP automation requests. The users can be set up with an access type of **`Read only`** or **`Read/write`**, providing some users more permission than others.

Common Information Model (CIM)

The system administrator can enable CIM automation support by using the **Customize API Settings** task. This enablement causes the HMC to accept inbound CIM requests on TCP ports 5988 and 5989. All CIM-based automation requests sent to the HMC must use SSL encryption with the same set of certificates as for remote user access. Additionally, each CIM request contains a user ID and password for authenticating the request. This user ID and password are validated by using the same set of user IDs and passwords for normal HMC user access, including LDAP authentication users. Similar to the role-based access control for regular HMC users, a CIM user can manage only the set of system resources and use only the tasks that are assigned to the user ID.

Note: Before HMC version 2.11.0, the **Customize Console Services** task is used to enable CIM automation.

Web Services

As with enabling SNMP automation, enabling web services automation support through the **Customize API Settings** task allows the HMC to accept incoming HTTP requests on TCP port 6794. The enablement can be limited to accept requests from specific IP addresses or all IP addresses. Each web services HTTP request contains authentication information that is used for authenticating the request. This information is validated against the same set of user IDs and passwords for normal HMC user access, including LDAP authentication users. Similar to the role-based access control for regular HMC users, web services requests are limited to only the set of system resources that are allowed for the user ID associated with the request.

Even with a valid user ID and password, the HMC accepts web services requests only from individual users who are explicitly granted access. In order for a user to access the web services APIs, the access administrator can use the **Customize API Settings** task enable access control for individual users. Alternately, the access administrator can use the **User Management** task to set the user to **`Allow access to Web Services management interfaces`**. Additionally, from the **User Management** task, the access administrator can also customize the maximum number of web services API sessions and idle web services API session timeout values for each user.

Operating System HMC Considerations

Many customers have strict controls with z/OS® in controlling which users have access to which z/OS commands. Enabling **Operating System Messages** on the HMC enables it for all HMCs that manage that system or LPAR. Thus, how you manage **Operating System Messages** enablement is an HMC security consideration. Consider the following items:

- Limit what HMCs can manage the system
- Limit which HMC users can access the LPAR
- Limit which HMC users can run the **Operating System Messages** task
  - Limit to read-only if read/write is not required
- For z/OS, use RACF® profiles to limit which commands can be entered by the system console. **Operating System Messages** commands are entered as if from the system console.
- For z/OS 2.1 or newer
  - Use the new HMC **Integrated 3270 Console** support
  - Use unique user logon/RACF controls for commands
- For z/VM and Linux on Support Elements accessed from the HMC, **Operating System Messages** requires a logging on with an OS user ID

Base Control Program internal interface (BCPii)

The Base Control Program internal interface (BCPii) allows authorized z/OS applications to have HMC-like control over systems in the process control (HMC) network. A set of robust APIs is provided for that

control from z/OS applications. In addition, BCPii provides complete communication isolation of existing networks (intranet/internet) from the process control (HMC) network. Communication to the support element is completely within base z/OS.

BCPii from z/OS is used for Sysplex Monitoring and Recovery controls and Graphically Dispersed Parallel Sysplex® (GDPS®). All systems in the Sysplex must be defined to the Change Management HMC.

The **Customize/Delete Activation Profiles** task provides additional BCPii permission control to indicate whether a logical partition can send and/or receive requests. The **Systems Details** task Security window controls whether to dynamically enable the system to receive commands from partitions.

For more information, see the *z/OS MVS™ Programming: Callable Services for High-Level Languages SA23-1377-02* publication.

Nucleus Initialization Program (NIP)

The HMC can be configured to be a Nucleus Initialization Program (NIP) console. An example is to choose to have only the NIP console on the HMC **Operating Systems Messages**. If there are no NIP consoles (that is, OSA, or 3274 control unit devices) specified in the I/O Definition File (IODF) or all of those NIP consoles are offline, z/OS automatically uses the system console (**Operating System Messages**) to receive z/OS IPL messages. The command `V CN(*),ACTIVATE` is not needed for commands to be accepted from the system console. When IPL is over, if there are z/OS operator consoles defined and online, z/OS uses them and the "system" console is deactivated. To continue use of the system console HMC **Operating System Messages**, the `V CN(*),ACTIVATE` command is required. If there are no z/OS operator consoles available, the system console continues to be used.

For more information, see the *z/OS V1R13 MVS Planning Operations* publication.

Service and support

The HMC provides the customer with both user and automation controls. Service representatives also use the HMC to perform service-related tasks to the HMC itself and to the associated system resources the HMC manages. Because customers have diverse needs, access permitted to service representatives has a wide range, from being treated like any other HMC user to being completely locked out of the HMC. The HMC provides the customer with the controls needed to designate service representative's access to the HMC.

Service and support access

One of the traditional user classifications is that of *service personnel*. By default the HMC is shipped with a default user ID of **SERVICE** for use by service personnel. The user roles that are associated with this default user evolved over time. Table 9 on page 25 lists the user roles that are assigned to default user **SERVICE** over various HMC versions.

*Table 9. Default user **SERVICE**'s resource and task roles*

HMC version 2.15.0	HMC version 2.14.0 and 2.14.1	HMC versions 2.11 and 2.12	HMC version 2.10 or prior
All System Managed Objects	All System Managed Objects	All zCPC Managed Objects	All Managed Objects
		All Directors/Timers Managed Objects	All Directors/Timers Managed Objects
		All Fiber Saver Managed Objects	All Fiber Saver Managed Objects
	BladeCenter Objects	BladeCenter Objects	
	DPXI50z Blade Objects	DPXI50z Blade Objects (version 2.12 only)	

*Table 9. Default user **SERVICE**'s resource and task roles (continued)*			
HMC version 2.15.0	**HMC version 2.14.0 and 2.14.1**	**HMC versions 2.11 and 2.12**	**HMC version 2.10 or prior**
	Ensemble Object	Ensemble Object	
	IBM Blade Objects	IBM Blade Objects	
	IBM Blade Virtual Server Objects	IBM Blade Virtual Server Objects	
		ISAOPT Blade Objects (version 2.11 only)	
		Service Fiber Saver tasks	Service Fiber Saver tasks
		Service Representative Director/Timer Tasks	Service Representative Director/Timer Tasks
Service Representative Tasks	Service Representative Tasks	Service Representative Tasks	Service Representative Tasks

This default setup provides service representatives with all the tasks needed to service the HMC and its associated system resources. This user is just like every other HMC user; that is, it can be altered or deleted to meet the security needs of the customer. Making radical changes in this area can affect IBM's ability to service the HMC and associated system resources, so any changes should be communicated to your service representative.

In addition to the service representative's normal usage of the HMC, there are rare cases where more detailed problem determination is required. For this reason, a special HMC user can be used by product engineering to perform in-depth problem determination. This user, **PEMODE**, differs from other HMC users in a couple ways:

- The customer cannot alter or delete this user
- The password for this user ID is unique for each HMC and changes daily.

The system administrator cannot manage this user like other users, but the HMC does provide the **Customize Product Engineering Access** task, which the customer can use to disable this user ID. Disabling product engineering access makes this user unusable, which prevents any unauthorized access to the HMC by product engineering. When product engineering access to the Hardware Management Console is authorized, the system administrator can decide whether product engineering can access the system remotely.

Note: The product engineering user ID requires the user to revalidate the password every 2 hours while it is being used.

Security Portal

System Integrity is IBM's commitment, designs, and development practices that are intended to prevent unauthorized application programs, subsystems, and users from bypassing system security; that is, to prevent them from gaining access, circumventing, disabling, altering, or obtaining control of key system processes and resources unless allowed by the installation.

A System Integrity vulnerability is defined as the ability of any program that is not authorized by a mechanism under the installation's control to circumvent or disable store or fetch protection, access a resource that is protected by a Security Server/Manager, or obtain control in an authorized state; that is, in supervisor state, with a protection key less than eight, or Authorized Program Facility (APF) authorized. If a System Integrity problem is reported, IBM always takes action to investigate, and if validated take appropriate action to resolve it. These actions might include development of fixes, identification of applicable workarounds, recommending migration to a later release, and so on.

Security vulnerabilities however, are defined as a set of conditions in the design, implementation, operation, or management of a product or service that is unable to prevent an attack by a party, which results in exploitation such as controlling or disrupting operation, compromising (that is, deleting, altering, or extracting) data, or assuming ungranted trust or identity. Examples might range from TCP/IP or Java architectural concerns, to things like Denial of Service (DoS) attacks, heuristic errors, or algorithm errors.

The Z mainframe makes available a Security Portal that allows clients to learn about the latest security and system integrity fixes available, which can help enable clients to keep their enterprise up to date. IBM uses several internal and external sources as input to the security and system integrity process to assist IBM as it investigates and works on vulnerabilities that might potentially affect Z mainframes.

If you are a customer, IBM provides access to the Security Portal intended to help you stay current with security and system integrity fixes. The portal provides current patch data and Associated Common Vulnerability Scoring System (CVSS) V2 ratings for new APARs. Security and integrity fixes are only created for supported versions of Z products.

To obtain access to the Security Portal, click **Portal Registration** on the *Enterprise security* web page at http://www.ibm.com/systems/z/solutions/security_subintegrity.html.

Remote support

One of the most important roles the HMC plays is being the connectivity point for communicating with IBM. For redundancy, one or more HMCs can be configured to act as this connectivity point. There are many reasons an HMC might need to communicate with IBM; some of them are as follows:

- To report problems that are detected by the HMC or detected by one or more of the managed system resources
- To transmit extra data IBM support needs for problem analysis
- To download firmware fixes for the HMC or managed system resources
- To report hardware inventory, system configuration, and system availability data
- To process OnDemand orders; customer orders that update Z mainframe capacity.

These actions are known as *call-home events*. The call-home events are transmitted to IBM by using the Remote Support Facility (RSF). RSF is designed to ensure that the security of your system and network is not compromised. The following security characteristics are in effect:

- Remote Support Facility requests are always initiated from the Hardware Management Console to IBM. An inbound connection is never initiated from the support system.
- All data that is transferred between the Hardware Management Console and the support system is encrypted in a high-grade Secure Sockets Layer (SSL) encryption.
- During SSL encrypted connection initialization, the Hardware Management Console validates the trusted host by its digital signature that is issued for the support system.
- Data sent to the support system consists solely of hardware problems and configuration data. No application or customer data is transmitted to IBM.
- The Hardware Management Console can be configured to use a second network card to physically separate a dedicated LAN connection from the Internet-enabled network.
- The Hardware Management Console audit log is updated each time that a connection is made with the support system.

A Support Element (SE) can call-home service events through any HMC (at its release level or higher) that is configured for outbound connectivity. The HMC can be configured as a call-home server when the CPC or zBX Node object is defined to the HMC with the **Add Object Definition** task. Alternately, the **Act as a call-home server** setting can be changed by using the **Change Object Definition** task. An HMC can call-home its own service events if it is configured for call-home. It is also eligible to use another HMC that is automatically discovered or is manually configured by using the **Customize Outbound Connectivity** task.

To avoid a single point of failure, it is recommended that each Support Element and Hardware Management Console are 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 by using the other available call-home servers until one is successful or all are tried.

The ability to call-home from the HMC to the support system requires HMC access to an external network. Planning is required to enable firewalls and evaluate your Network security policy. Details of the implementation of the Remote Support Facility are available in the *Integrating the Hardware Management Console's Broadband Remote Support Facility into your Enterprise*, SC28-6986. You can find this publication in the **Library** section of Resource Link (www.ibm.com/ servers/resourcelink).

The HMC can use various methods for communicating to IBM. This fact allows the system administrator to choose the communication method that matches the customer environment and requirements. The following sections outline different Internet connectivity configurations in more detail.

Internet connectivity

In this configuration, the HMC uses a client-provided Internet connection to connect to the support system. All the communications are handled through TCP sockets (which always originate from the HMC) and use SSL to encrypt the data that is being sent back and forth.

The network interface of the HMC that provides this Internet connectivity should **not** be the same one used for connectivity to the system resources managed by the HMC. This restriction is easily accomplished because the HMC provides multiple network interfaces, one of which can be used for Internet connectivity and another for managing the system resources.

Optionally, the HMC can also be enabled to connect to the Internet through a client-configured proxy server.

A configured outbound connectivity connection flows over the console's default gateway to the Internet. In order for the console to successfully use the Internet, the following items must be properly configured in the **Customize Network Settings** task:

- The console must have a Local Area Network (LAN) adapter that is connected to a network with Internet access. This connection 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).
- Transmission that uses the enhanced support system requires a Domain Name Server (DNS) to be configured on your console, unless the connection is through an SSL proxy that has a DNS configured.

Without proxy server

The following diagram shows the HMC connecting to IBM without a proxy server.

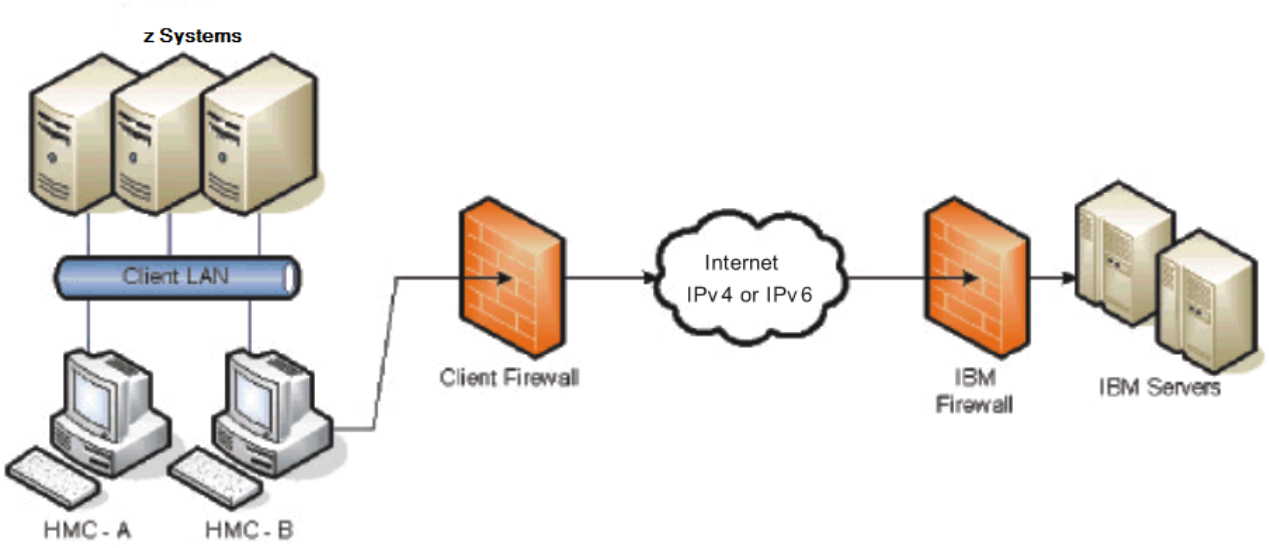


Figure 1. Z mainframes connectivity to IBM - Without a proxy server

In this setup, the HMC connects through the client-provided Internet connection by the default route. For this type of configuration, the client should use a second network card to physically separate the local system network from the Internet-enabled network.

For the HMC to communicate successfully, the client's external firewall must allow established TCP packets to flow freely on port 443. The use of Source Network Address Translation (SNAT) and masquerading rules to mask the HMC's source IP address are both acceptable. The firewall can also limit the specific IP addresses to which the HMC can connect. Table 10 on page 31 contains the list of IP addresses.

With proxy server

The following diagram shows the HMC connecting to IBM by using a client-provided proxy server.

Figure 2. Z mainframes connectivity to IBM - With a proxy server

To forward SSL sockets, the proxy server must support the basic proxy header functions (as described in RFC (Request for Comments) #2616) and the CONNECT method. Optionally, basic proxy authentication

(RFC #2617) can be configured so that the HMC authenticates before it attempts to forward sockets through the proxy server.

For the HMC to communicate successfully, the client's proxy server must allow connections to port 443. The proxy server can also limit the specific IP addresses to which the HMC can connect. Table 10 on page 31 contains the list of IP addresses.

Modem connectivity

Although modem connectivity is supported in version 2.11.1 or earlier, IBM recommends a configuration that uses Internet connectivity. Internet connectivity provides faster service because of the large size of error data files that might be sent to the support system.

The following diagram shows a typical dial environment. This configuration allows the HMC to use a modem to dial the AT&T global network and connect to the service delivery center. The HMC automatically detects the modem when it starts.

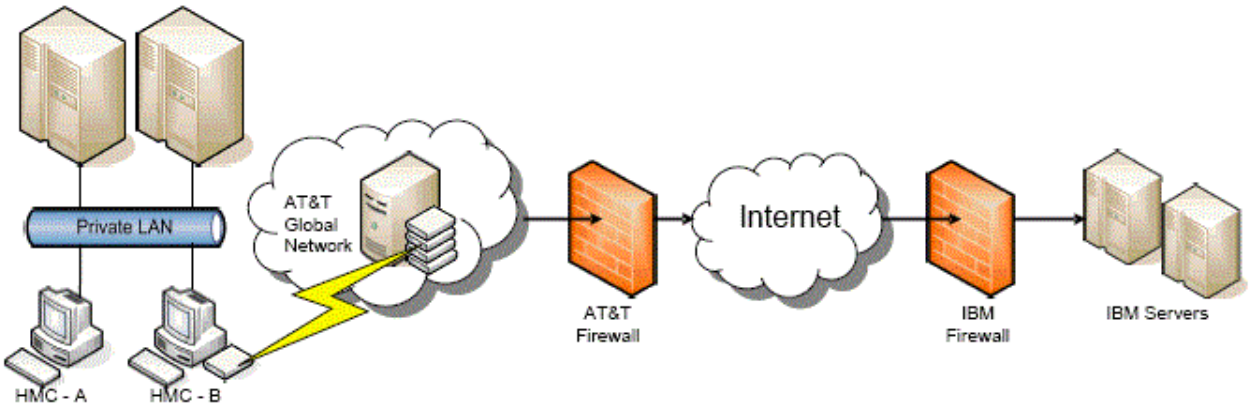


Figure 3. Z mainframe - Modem connectivity

In this scenario, the HMC uses one of the configured phone numbers to dial the modem, connecting to the AT&T Global Network. After the modem connects, the HMC authenticates itself and establishes a Point-to-Point Protocol (PPP) session between the two modems. Finally, after the PPP session finishes, AT&T allows IP connections through a *Fenced Internet*, which completes the network between the HMC and the IBM service delivery center.

All the communications between the HMC and the IBM systems are handled through TCP sockets. These sockets always originate from the HMC and use Secure Sockets Layer (SSL) to encrypt the data that is being sent back and forth.

The Fenced Internet connection uses a firewall to limit access between the HMC and the Internet. Specifically, it limits communication to HMC-initiated connections to the authorized IBM IP addresses needed to connect to the service delivery center.

IBM system address lists

The HMC uses *Internet Connectivity Addresses* when it is configured for Internet connectivity. All connections to these IP addresses use port 443 TCP. If a firewall is in place between the console (or SSL proxy) and the Internet, it must allow outgoing TCP/IP connections on port 443 from the Hardware Management Console (or SSL proxy) to the Service Support System. The IP addresses you must allow depends on the protocol you chose on the **Internet Protocol** selection field.

Internet connectivity to the support system is enhanced to enable access from the IPv6 Internet as well as the IPv4 Internet. If you require access to the support system that uses the IPv6 Internet, you must allow access to all of the IPv6 addresses.

Table 10. Internet connectivity addresses. HMC uses IP addresses when it is configured for Internet connectivity.

Americas and Non-Americas - IPv4	**Americas and Non-Americas - IPv6**
• 129.42.26.224 • 129.42.34.224 • 129.42.42.224 • 129.42.50.224 • 129.42.54.189 (enhanced) • 129.42.56.189 (enhanced) • 129.42.58.189 (enhanced) • 129.42.60.189 (enhanced)	• 2620:0:6c0:1::1000 • 2620:0:6c1:1::1000 • 2620:0:6c2:1::1000 • 2620:0:6c4:1::1000 • 2620:0:6c0:200:129:42:54:189 (enhanced) • 2620:0:6c0:200:129:42:56:189 (enhanced) • 2620:0:6c1:200:129:42:58:189 (enhanced) • 2620:0:6c2:200:129:42:60:189 (enhanced)

If an SSL Proxy is used to access the Internet, you can configure the Hardware Management Console to send an HTTP Connect request to the proxy with either the IP address (as shown above), or using a host name. If you configure it to use a host name, your proxy must accept connections to port 443 on the following host names:

- www-945.ibm.com
- esupport.ibm.com (enhanced)

Chapter 5. Logging and audit trails

When the security characteristics of a computer system like the HMC are understood and trusted, facilities must be in place to monitor and audit the security of the system to ensure that it is operating correctly. For this reason, the HMC uses its *security log* to record important security-related events. The customer can use the **View Security Logs** task to view these security events and the **Archive Security Logs** task to offload security logs for storage.

The security log contains entries for security-related events. A short list that illustrates the types of events that are contained in the security log is as follows:

- User logon or logoff
- Failed logon attempts
- Password changes
- Creation, deletion, and alteration of users
- Creation, deletion, and alteration of user roles
- Creation, deletion, and alteration of Z mainframe activation profiles
- Processing of disruptive commands
- Change management activity
- Network traffic that is blocked by the firewall.

The customer is intended to use the security log to determine when events occurred that altered the security characteristics of the HMC. The security log might indicate an action that might have security implications to the HMC or the system resources that it manages. The **View Security Logs** task allows the customer to search the open log by date, event, category, or new in version 2.13.0, by user. This search capability limits the list of entries to just what is of particular interest.

For auditing purposes, the **Audit and Log Management** task generates a report that can be viewed and offloaded to a remote workstation or removable media. There is various data types (such as Configuration, Security Log, or User profiles) that can be chosen to tailor the report. A range of dates and times can also be entered to limit the report to a specific period. A range of dates and times can also be entered to limit the report to a specific time.

Event Monitoring

The **Monitor System Events** task allows the creation and management of event monitors. An *event monitor* listens for events from managed objects. When an event is received, the monitor tests it with user-defined time and text filters. If the event passes the tests, the monitor enables an email to be sent to interested users. This function requires a Simple Mail Transfer Protocol (SMTP) server that must be accessible from the HMC.

Customers might want to use the **Monitor System Events** task to automate notification of certain critical security log events. In this case, system programmers and system administrators need not manually monitor the security log as frequently.

Chapter 6. Best practices

While the needs of each customer installation are different and the following best practices might not be feasible at every installation, they can still be used as an outline of considerations for ensuring the HMC and the associated system resources are secure.

The following practices are listed in the order in which they provide security for the HMC. This list does not mean that items that are later in the list diminish security but rather that they introduce extra security considerations for the customer. For example, not allowing remote access to the HMC is more secure than allowing it because an entire set of network communications does not occur. This practice does not mean that remote access to the HMC is insecure. It is, in fact, secure, but it introduces a security consideration that the customer must address.

Physical security

- Make sure the Z mainframe and other system resources are physically located in a secure location. The location should be an area that has physical access controlled and monitored, such as a raised floor.
- When possible, install the HMC in the same type of physically secure environment as previously described for the system resources.

Network security

- Connect the Z mainframe and other resources only to a dedicated, physically separate network; for example, connect all system resources on a dedicated raised floor network.
- Connect the HMC to the previously described dedicated system resources network. If connectivity to the HMC from other networks in the customer's enterprise is needed, provide this connectivity by connecting the second HMC network adapter to the appropriate customer network. (Remember: the HMC never routes network traffic, so the dedicated Z mainframe network is still secure and isolated.)
- Disable the **SSLv3 and RC4 compatibility** service on all HMCs and SEs after the current MCLs are applied to all systems.
- Ensure the HMC is not directly accessible from the Internet. If connectivity from outside an Intranet is required, utilize a VPN or similar solution to secure that connection. Utilizing such safeguards helps protect against future unknown malicious attacks.

Automated operational control

- Unless required, make sure that all automation interfaces of the HMC are disabled. If automation is required, then make sure to configure each of these interfaces in a secure manner (for example, do not use common authentication tokens or world-write types of access).
- If you use SNMP automation, use SNMPv3 utilizing its more secure authentication.
- Use Web Services automation, which allows for more granularity by having individual user authority. The users who are granted specific authority can use the Web Services interface.

User operational control

- To prevent the HMC from being logged on while unattended, make sure that the automatic logon capability of the HMC is not enabled.

Remote user access

- Unless required, make sure that remote access to the HMC is disabled.
- If remote access is required, make sure to allow remote access only for the specific users that require this type of access

- Use CA signed certificates
- Use TLS cipher suites of high strength
- Ensure browser levels are up-to-date and security fixes applied.

Users

- At a minimum, change the passwords for all the default HMC users. A more secure approach is to copy the default users to define a user for each individual user of the HMC and then remove all of the default users.
- Do not share HMC users among multiple people.
- Customers should ensure they have redundant administrative users for each console.
- Customers should document contact information and/or procedures using the *Welcome Text* so that service personnel know how to engage customer administrative if the HMC/SE access is needed.

Passwords

- Define password rules that adhere to the guidelines for the customer enterprise and make sure that each user is configured to use these password rules. If no guidelines exist, then make sure that each user is configured to use the Standard password rule (previously described).

User roles

- Make sure that each user is granted access only to the tasks and managed resources that are needed to perform job responsibilities.

Data replication

- Use data replication to ensure that User Profile information (users, roles, password rules, and so forth) is automatically synchronized among all HMCs installed in the enterprise.

Secure FTP

- Utilize secure FTP for the HMC offload and import functions.

Logging and audit trails

- Implement procedures that offload and analyze the HMC security logs for any suspicious activity.
- When feasible, automate notification of security log events for the HMC.

Security Portal

- Stay current with security and system integrity fixes by registering for the Security Portal.

Chapter 7. Executive summary

The HMC is a PC-based appliance or 1U server that is designed for the operational control of system resources, such as servers and the operating systems that run on them, Director/Timer Consoles, and Fiber Savers. The HMC Licensed Internal Code application controls all access to the HMC and the tasks that are used for these system resources, and no access is provided to the underlying operating platform of the HMC appliance.

By default, all HMC security-related settings (for example, remote user access) are disabled to prevent inadvertent security exposures. In addition to operational controls, the HMC can also act as a single point of control for automation. As previously stated, the system administrator must explicitly enable and configure optional features such as this automation before they can be used.

The HMC provides a myriad of controls for managing users, passwords, user roles, certificates, and so forth, in addition to the physical security settings the HMC's PC hardware provides. Where possible, SSL-based encryption is performed on all data for all network connections into and out of the HMC. In addition, the HMC provides audit trails for security-related events in the form of security logs or audit logs from which various reports can be generated. The logs can also be offloaded for storage purposes.

Appendix A. HMC versions

HMC version 2.15.0 supports z15, 2.14.1 and version 2.14.0 supports z14™, 2.13.1 supports z13s®, version 2.13.0 supports z13®, zBX Node, and the legacy systems that are listed in the following table.

Table 11. HMC/SE versions for various machine types

Machine Family	Machine Type	Firmware Driver	HMC/SE Version	Ensemble Node Potential
z15	8561	41	2.15.0	No
z14	3907	36	2.14.1	Yes
z14	3906	32	2.14.0	Yes
z13s	2965	27	2.13.1	Yes
z13	2964	22	2.13.0	Yes
zBX Node	2458 Mod 004	22	2.13.0	Required
zBC12	2828	15	2.12.1	Yes
zEC12	2827	15	2.12.1	Yes
z114	2818	93	2.11.1	Yes
z196	2817	93	2.11.1	Yes
z10 BC	2098	79	2.10.2	No
z10 EC	2097	79	2.10.2	No
z9 BC	2096	67	2.9.2	No
z9 EC	2094	67	2.9.2	No

Note: z900/z800 (Driver 3G, SE version 1.7.3) & z990/z890 (Driver 55, SE version 1.8.2) systems are no longer supported.

Appendix B. Notices

This information was developed for products and services offered in the US.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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 jurisdictions 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 provide in any way it believes appropriate without incurring any obligation to you.

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.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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 actual people or business enterprise is entirely coincidental.

Trademarks

IBM, the IBM logo, and 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.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Class A Notices

The following Class A statements apply to this IBM product. The statement for other IBM products intended for use with this product will appear in their accompanying manuals.

Federal Communications Commission (FCC) Statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 2014/30/EU on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55032. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

European Community contact:
IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 (0) 800 225 5423 or +49 (0) 180 331 3233
email: halloibm@de.ibm.com

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

VCCI Statement - Japan

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

The following is a summary of the Japanese VCCI statement above:

This is a Class A product based on the standard of the VCCI Council. If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

Japan JIS C 61000-3-2 Compliance

（一社）電子情報技術産業協会 高調波電流抑制対策実施
要領に基づく定格入力電力値： Knowledge Centerの各製品の
仕様ページ参照

For products less than or equal to 20 A per phase, the following statement applies:

高調波電流規格 JIS C 61000-3-2 適合品

For products greater than 20 A, single-phase, the following statements apply:

高調波電流規格 JIS C 61000-3-2 準用品

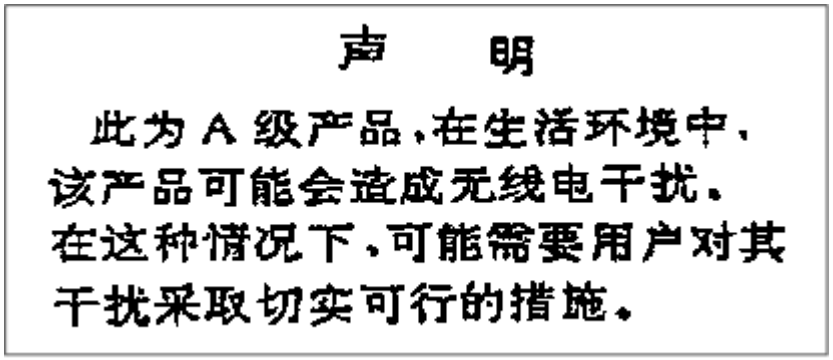
本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
回路分類：6（単相、ＰＦＣ回路付）
換算係数：0

For products greater than 20 A per phase, three-phase, the following statements apply:

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
回路分類 ：5（3相、ＰＦＣ回路付）
換算係数 ：0

Electromagnetic Interference (EMI) Statement - People's Republic of China



Declaration: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may need to perform practical action.

Electromagnetic Interference (EMI) Statement - Taiwan

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。

The following is a summary of the Taiwan EMI statement above:

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.

IBM Taiwan Contact Information:

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Electromagnetic Interference (EMI) Statement - Korea

이 기기는 업무용(A급)으로 전자파적합등록을 한 기기이오니
판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의
지역에서 사용하는 것을 목적으로 합니다.

Germany Compliance Statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55032 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

EN 55032 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2014/30/EU) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 (0) 800 225 5423 or +49 (0) 180 331 3233
email: halloibm@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55032 Klasse A.

Electromagnetic Interference (EMI) Statement - Russia

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

Index

N

O

P

R

S

T

U

V

W

Z

SC28-6987-02