Managing the Hardware Management Console (HMC)
Managing the Hardware Management Console (HMC)
Before using this information and the product it supports, be sure to read the information in "Notices," on page 95 and the manual *IBM eServer Safety Information*, G229-9054.
# Contents

## Chapter 1. Managing the Hardware Management Console (HMC)

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
</tbody>
</table>

## Chapter 2. Printable PDF

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
</tr>
</tbody>
</table>

## Chapter 3. HMC concepts

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
</tr>
</tbody>
</table>

- Implementations of HMCs
- HMC user interface
  - Navigation area
  - Contents area
  - Menu bar
  - Toolbar
  - Status bar
  - HMC applications
- Tasks and roles
  - Definitions of HMC roles
  - HMC configuration tasks
  - HMC user management tasks
- Predefined passwords for hscroot and root user IDs
- HMC network connections
  - Types of HMC network connections
  - Private and open networks in the HMC environment
  - The HMC as a DHCP server
- Web-based System Manager Remote client
  - Installation requirements for the remote client
  - Remote client comparison
  - System Manager Security

## Chapter 4. Setting up the HMC

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
</tr>
</tbody>
</table>

- Cabling the HMC
- Installing the HMC into a rack
- Installing the external modem into a rack
- Identifying the Ethernet port defined as eth0
- Gathering required configuration settings
- Configuring the HMC
  - Configuring the HMC using the fast path through the Guided Setup wizard
  - Configuring the HMC using the Guided Setup wizard
    - Accessing the Guided Setup wizard using the HMC interface
    - Configuring the HMC using the HMC configuration checklist
    - Changing the predefined passwords for hscroot and root user IDs
- Configuring network connections
  - Configuring LAN adapters
  - Setting the media speed
  - Selecting the network type
  - Configuring the HMC as a DHCP server
  - Setting the IP address
  - Changing HMC firewall settings
  - Setting identification information
  - Configuring a routing entry as the default gateway
  - Configuring domain name services
  - Configuring domain suffixes
  - Testing the connection between the HMC and the managed system
  - Postconfiguration steps for the HMC

## Chapter 5. Installing and securing the remote client

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>85</td>
</tr>
</tbody>
</table>

- Configuring one HMC as a certificate authority
- Generating private key ring files for the servers
- Installing private key ring files on the servers
- Distributing the certificate authority’s public key with Web-based System Manager Remote Client for Java Web Start
- Distributing the certificate authority’s public key with Web-based System Manager Remote Client
- Viewing configuration properties
- Configuring HMC object manager security
- Installing the Web-based System Manager Remote Client
- Uninstalling the Web-based System Manager Remote Client
- Installing the Web-based System Manager Remote Client for Java Web Start
- Uninstalling the Web-based System Manager Remote Client for Java Web Start

## Chapter 6. Working with the HMC

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>73</td>
</tr>
</tbody>
</table>

- Basic operations
- Starting the HMC
- Shutting down, rebooting, and logging off the HMC
- Setting the date and time
- Changing the HMC interface language
- Configuring the HMC keyboard layout
- Viewing recent HMC activity
- Working with partition profile information
- Backing up partition profile data
- Initializing profile data
- Restoring profile data
- Removing profile data
- Backing up and restoring the HMC
- Backing up critical HMC data
- Restoring critical HMC data
- Restoring from DVD
- Restoring from a remote server
- Scheduling and reviewing HMC backups
- Saving HMC upgrade data
- Reinstalling the HMC machine code
- Working with users, roles, and passwords
- Creating an HMC user
- Viewing an HMC user description
- Copying HMC user information

© Copyright IBM Corp. 2004, 2005
Deleting an HMC user. 82
Creating a customized HMC role 82
Editing HMC user information and roles 82
Changing HMC user passwords 82
Using the HMC remote command line 83
Viewing HMC remote command information 83
Setting up secure script execution between SSH clients and the HMC 83
Enabling and disabling HMC remote commands 84

Chapter 7. Troubleshooting HMC setup 87

Chapter 8. Related information 93

Appendix. Notices 95
Trademarks 96
Communications statements 96
Federal Communications Commission (FCC) statement 97
Federal Communications Commission (FCC) statement 99
Terms and conditions for downloading and printing information 100
Product recycling and disposal 101
Battery return program 101
IBM Cryptographic Coprocessor Card Return Program 101
Chapter 1. Managing the Hardware Management Console (HMC)

You can manage IBM® eServer™ i5 and eServer p5 servers, logical partitions, and Capacity on Demand with the Hardware Management Console (HMC). The HMC communicates with systems using service applications to detect, consolidate, and send information to IBM for analysis.

Use the following information to help you set up the HMC:

**Chapter 2, “Printable PDF,” on page 3**
Print a PDF of the setup instructions for the HMC.

**Chapter 3, “HMC concepts,” on page 5**
Learn about the different types of HMCs, predefined passwords, installation methods for the remote client, installation requirements for the remote client, and System Manager Security.

**Chapter 4, “Setting up the HMC,” on page 25**
Cable and configure the HMC. This includes installing the HMC into a rack and configuring network connections, security, and service applications.

**Chapter 5, “Installing and securing the remote client,” on page 65**
Install the Web-based System Manager Remote Client or install the Web-based System Manager Remote Client for Java™ Web Start.

**Chapter 6, “Working with the HMC,” on page 73**
Describes how to perform actions that pertain to the HMC itself.

**Chapter 7, “Troubleshooting HMC setup,” on page 87**
Troubleshoot common HMC setup problems.

**Chapter 8, “Related information,” on page 93**
View and print information related to the Adding the HMC topic collection.
Chapter 2. Printable PDF

To view or download the PDF version of this document, select Managing the Hardware Management Console (about 1628 KB).

Saving PDF files

To save a PDF on your workstation for viewing or printing:
1. Right-click the PDF in your browser (right-click the link above).
2. Click Save Target As... if you are using Internet Explorer. Click Save Link As... if you are using Netscape Communicator.
3. Navigate to the directory in which you would like to save the PDF.
4. Click Save.

Downloading Adobe Acrobat Reader

You need Adobe Acrobat Reader to view or print these PDFs. You can download a copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html).
Chapter 3. HMC concepts

The following topics provide essential supporting information to the tasks of setting up the Hardware Management Console (HMC) and installing the remote client:

“Implementations of HMCs”
Learn about the local HMC, the remote HMC, and the Web-based System Manager Remote Client.

“HMC user interface” on page 6
Learn about the HMC graphical user interface.

“Tasks and roles” on page 9
Understand the user roles that can be assigned to each HMC user. Learn about the tasks that each HMC user role can perform and the commands associated with each task.

“Predefined passwords for hscroot and root user IDs” on page 14
Learn about the user IDs and passwords included with the HMC.

“HMC network connections” on page 14
Understand how the HMC can be used in a network.

“Web-based System Manager Remote client” on page 20
This is my description of this link.

Implementations of HMCs

The Hardware Management Console (HMC) is a system that controls managed systems, including IBM eServer hardware, logical partitions, and Capacity on Demand. To provide flexibility and availability, there are different ways to implement HMCs, including the local HMC, remote HMC, redundant HMC, and the Web-based System Manager Remote Client. Figure 1 on page 6 illustrates how HMCs might be implemented in your network.

Local HMC
A local HMC is any physical HMC that is directly connected to the system it manages through a private service network. An HMC in a private service network is a DHCP server from which the managed system obtains the address for its firmware. Additional local HMCs in your private service network are DHCP clients.

Remote HMC
A stand-alone HMC or an HMC installed in a rack that is used to remotely access another HMC. A remote HMC may be present in an open network.

Redundant HMC
A redundant HMC manages a system that is already managed by another HMC. When two HMCs manage one system, those HMCs are peers and can be used simultaneously to manage the system. The redundant HMC in your private service network is usually a DHCP client.

Web-based System Manager Remote Client
The Web-based System Manager Remote Client is an application that is usually installed on a PC. You can then use this PC to access other HMCs remotely. Web-based System Manager Remote Clients can be present in private and open networks. You can perform most management tasks using the Web-based System Manager Remote Client.

The remote HMC and the Web-based System Manager Remote Client allow you the flexibility to access your managed systems (including HMCs) from multiple locations using multiple HMCs.
For more information about how you can plan for and implement HMCs, see Solutions with the Hardware Management Console (HMC).

Figure 1. Implementations of HMCs

**HMC user interface**

The following components make up the HMC graphical user interface (GUI):

“Navigation area” on page 7
Learn about the navigation area of the HMC GUI.
“Contents area”
Learn about the contents area of the HMC GUI.

“Menu bar”
Understand the menu bar on the HMC GUI.

“Toolbar” on page 8
Learn about the toolbar on the HMC interface.

“Status bar” on page 8
Learn about the status bar on the HMC GUI.

“HMC applications” on page 8
Understand the HMC folders and applications.

The HMC also provides a pop-up menu (also called the context menu) for quick access to menu choices. The pop-up menu lists the actions found in the Selected and Object menus for the current object or objects.

Navigation area
The left side of the HMC graphical user interface (GUI) is the Navigation area. It displays a hierarchy of items ordered in a tree structure. The root of the tree is the Management Environment, which contains the name of the HMC into which you are currently logged. This name is the same as the host name that you have given the HMC.

The Management Environment is a set of host systems that can be managed from the HMC. The host systems can be the HMC into which you are currently logged and other remote HMCs.

Each folder in the Navigation area contains different HMC applications used in the specific management task, such as the Server and Partition folder. If you select one of these HMC applications, it provides appropriate submenus and objects in the Contents area.

Contents area
The right side of the HMC graphical user interface (GUI) is called the Contents area. It displays managed objects and related tasks. You can select different views in the Contents area: large icons, small icons, or details in the form of a list.

Menu bar
The following menu items are provided in the menu bar of the HMC GUI:

Console
The Console menu contains choices that control the console. It enables you to add and remove managed systems, other HMCs, or other systems from the management environment. It also enables you to change themes on the desktop, change font sizes, open an outbound Telnet terminal session using an IP address or a host name, and exit the console.

Object
The title of the Object menu changes to indicate the type of resource managed by the current HMC application. For example, when the Server Management application is selected, the Object menu title becomes Server Management. The Object menu contains general choices and actions for an HMC application that do not require the selection of specific objects to act on. The find function is also located in the Object menu. The contents of the Object menu are updated when a new HMC application is selected.

Selected
The Selected menu contains the set of actions that are applicable to the object selected in the
Contents pane. The contents of the Selected menu are updated based on which object you select. The Selected menu is disabled when Overview and Launch applications are loaded. The open tab in the Selected menu expands the view of a managed system in the Navigation area.

**View**  
The View menu contains choices for navigating. It also includes choices for customizing the console in the Show submenu. For example, you can select to show or hide the toolbar and status bar. This menu also includes options that control how objects are presented. For example, if the Contents area content provides a choice of views, such as Large Icon, Small Icon, Details, and Tree, these choices are listed here. If the content has only a single view, no view choices are listed. When the content displays an icon or details view, the View menu includes choices for sorting and filtering the container.

**Window**  
The Window menu contains actions for managing subpanels in the console workspace. The new virtual terminal creates a new console subpanel in the workspace. Other choices control how all console subpanels are presented.

**Help**  
The Help menu lists user assistance choices. Different options enable you to view help contents, search for help on a particular topic, and view help information about shortcut keys.

**Toolbar**  
The toolbar of the HMC GUI lists commonly used actions that are available when the current plug-in application is loaded. It includes navigation controls, Find and View choices (if available), and a refresh option of the HMC GUI. The toolbar also provides tooltip help when the pointer remains over a toolbar icon for a few seconds.

**Status bar**  
The status bar of the HMC GUI displays at the lower edge of a console panel. It can be hidden or shown by clearing or checking the Status Bar option in the Show submenu under View. The status bar has the following fields ordered from left to right for displaying status information:

- **Padlock icon**  
The padlock icon is open when secure communications are not active.

- **Application loading status**  
When an HMC application is loaded, the text Ready displays. When an application is in the process of loading, a graphical bar is displayed.

- **Number of objects visible in the Contents area**  
Objects can be present on the managed system but hidden from the view by the view filter.

- **Number of objects selected in the Contents area**  
This field displays the number of objects that you have selected in the Contents area.

- **Security context**  
This field displays the administrator user name and the HMC host name for the currently active HMC.

**HMC applications**  
Application folders and application icons are provided in the Navigation area in the HMC GUI. The folders and icons contain several applications to be used for different system management tasks on the HMC and managed systems.

**HMC Management**  
This folder contains the HMC configuration and HMC Users applications. Use the HMC configuration application to do the following:

- **Set the HMC date and time**  
For more information about setting the HMC date and time, see [“Setting the date and time” on page 74](#).
• Configure and test network settings
  For more information about configuring network settings, see “Configuring the HMC using the HMC configuration checklist” on page 58.

• View console events
  For more information about viewing console events, see “Viewing recent HMC activity” on page 76.

• Schedule routine backups
  For more information about scheduling backups, see “Backing up and restoring the HMC” on page 78.

• Enable and disable remote commands and virtual terminals.

Use the HMC Users application to manage HMC users. For more information about managing users, see “Basic operations” on page 73.

Information Center and Setup Wizard
The Information Center and Setup Wizard application allows you to open the technical documentation for your server. The Setup Wizard helps you configure the HMC to work with the managed system.
For more information about configuring the HMC using the Setup Wizard, see “Configuring the HMC using the Guided Setup wizard” on page 56.

Licensed Internal Code Maintenance
The Licensed Internal Code Maintenance application folder contains the HMC Code Update and Licensed Internal Code Updates applications.
For more information about using these applications to maintain the code on your systems, see Getting fixes.

Server and Partition
The Server and Partition folder contains the Server and Frame Management applications. The Server Management application provides all logical partition-related tasks. It is used to create, maintain, activate, and delete logical partitions. This application also provides a focal point for all managed-system related tasks, such as powering the managed system on and off. The Frame Management application provides frame Bulk Power Assembly (BPA)-related tasks. It can be used to update managed frame passwords. This application can also be used to add, initialize, reset, remove, and view properties of managed frames.
For more information about logical partitions, see Partitioning the server.
For more information about working with the managed system and frame, see Working with managed systems and frames.

Service Applications
This folder contains several applications to be used for service-related tasks.
For more information about using these applications, see Customer service and support.

Tasks and roles
The following topics provide essential information regarding HMC roles and various configuration and user management tasks that can be performed:

“Definitions of HMC roles” on page 10
Describes the HMC roles that can perform various tasks.

“HMC configuration tasks” on page 10
Describes HMC configuration tasks and the roles that can perform them.

“HMC user management tasks” on page 12
Describes HMC user management tasks and the roles that can perform them.
Definitions of HMC roles

Each HMC user can be a member of a different role. Each of these roles allows the user to access different parts of the HMC and perform different tasks on the managed system. HMC roles are either predefined or customized.

The roles discussed in this section refer to HMC users; operating systems running on logical partitions have their own set of users and roles.

When you create an HMC user, you must assign that user a task role. Each task role allows the user varying levels of access to tasks available on the HMC interface.

For more information about the tasks each HMC user role can perform and the commands associated with each task, see Overview of HMC tasks.

You can assign managed systems and logical partitions to individual HMC users. This allows you to create a user that has access to managed system A but not to managed system B. Each grouping of managed resource access is called a managed resource role.

To learn more about managed resource roles and how to create them, refer to the HMC interface help.

Predefined HMC roles

The predefined HMC roles, which are the default on the HMC, are as follows:

**super administrator**
The super administrator acts as the root user, or manager, of the HMC system. The super administrator has unrestricted authority to access and modify most of the HMC system.

**service representative**
A service representative is an employee who is at your location to install, configure, or repair the system.

**operator**
An operator is responsible for daily system operation.

**product engineer**
A product engineer assists in support situations, but cannot access HMC user management functions. To provide support access for your system, you must create and administer user IDs with the product engineer role.

**viewer**
A viewer can view HMC information, but cannot change any configuration information.

Customized HMC roles

You can create customized HMC roles by modifying predefined HMC roles. Creating customized HMC roles is useful for restricting or granting specific task privileges to a certain user.

For more information about creating customized HMC roles, see "Creating a customized HMC role" on page 82.

HMC configuration tasks

Use the following table for descriptions of the HMC configuration tasks, the associated commands, and the user roles necessary to perform them.
<table>
<thead>
<tr>
<th>Task</th>
<th>Associated command</th>
<th>Roles</th>
</tr>
</thead>
</table>
| Add or remove an entry in the HMC syslog configuration file | chhmc              | super administrator: X  
|                                            |                    | service representative: X  
|                                            |                    | operator: X  
|                                            |                    | product engineer: X  
|                                            |                    | viewer: X  |
| Add or remove an entry in the HMC network time protocol configuration file | chhmc              | super administrator: X  
|                                            |                    | service representative: X  
|                                            |                    | operator: X  
|                                            |                    | product engineer: X  
|                                            |                    | viewer: X  |
| Back up critical console data              | bkconsdata         | super administrator: X  
|                                            |                    | service representative: X  
|                                            |                    | operator: X  
|                                            |                    | product engineer: X  
|                                            |                    | viewer: X  |
| Configure whether keyboard mapping configuration will occur during the next HMC reboot | chhmc              | super administrator: X  
|                                            |                    | service representative: X  
|                                            |                    | operator: X  
|                                            |                    | product engineer: X  
|                                            |                    | viewer: X  |
| Display the HMC BIOS level                | lshmc              | super administrator: X  
|                                            |                    | service representative: X  
|                                            |                    | operator: X  
|                                            |                    | product engineer: X  
|                                            |                    | viewer: X  |
| Display the HMC configuration              | lshmc              | super administrator: X  
|                                            |                    | service representative: X  
|                                            |                    | operator: X  
|                                            |                    | product engineer: X  
|                                            |                    | viewer: X  |
| Display the HMC network settings           | lshmc              | super administrator: X  
|                                            |                    | service representative: X  
|                                            |                    | operator: X  
|                                            |                    | product engineer: X  
|                                            |                    | viewer: X  |
| Display the HMC remote access settings     | lshmc              | super administrator: X  
|                                            |                    | service representative: X  
|                                            |                    | operator: X  
|                                            |                    | product engineer: X  
|                                            |                    | viewer: X  |
| Display the HMC VPD information            | lshmc              | super administrator: X  
|                                            |                    | service representative: X  
|                                            |                    | operator: X  
|                                            |                    | product engineer: X  
|                                            |                    | viewer: X  |
| Display the HMC version information        | lshmc              | super administrator: X  
|                                            |                    | service representative: X  
|                                            |                    | operator: X  
|                                            |                    | product engineer: X  
|                                            |                    | viewer: X  |
| Display the status of prompting for the Terms and Conditions agreement at user login | lsusrtca           | super administrator: X  
|                                            |                    | service representative: X  
|                                            |                    | operator: X  
|                                            |                    | product engineer: X  
<p>|                                            |                    | viewer: X  |</p>
<table>
<thead>
<tr>
<th>Task</th>
<th>Associated command</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable or disable displaying the Terms and Conditions agreement at user login</td>
<td>chusrtea</td>
<td>X</td>
</tr>
<tr>
<td>Install corrective service on the HMC</td>
<td>updhlmc</td>
<td>X  X X X X X</td>
</tr>
<tr>
<td>Modify the HMC configuration</td>
<td>chhmc</td>
<td>X  X X X X X</td>
</tr>
<tr>
<td>Modify the HMC network settings</td>
<td>chhmc</td>
<td>X  X X X X X</td>
</tr>
<tr>
<td>Modify the HMC remote access settings</td>
<td>chhmc</td>
<td>X  X X X X X</td>
</tr>
<tr>
<td>Reboot the HMC</td>
<td>hmcshutdown</td>
<td>X  X X X X X</td>
</tr>
<tr>
<td>Shut down the HMC</td>
<td>hmcshutdown</td>
<td>X  X X X X X</td>
</tr>
<tr>
<td>Update code on the HMC</td>
<td>updhlmc</td>
<td>X  X X X X X</td>
</tr>
<tr>
<td>View console events logged by the HMC</td>
<td>lssvcevents</td>
<td>X  X X X X X</td>
</tr>
</tbody>
</table>

For more information about how to perform HMC configuration tasks, see Chapter 6, “Working with the HMC,” on page 73. For more information on using commands, see “Using the HMC remote command line” on page 83.

**HMC user management tasks**

Use the following table for descriptions of the HMC user management tasks, the associated commands, and the user roles necessary to perform them.

<table>
<thead>
<tr>
<th>Task</th>
<th>Associated command</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a user for the HMC</td>
<td>mkhmcusr</td>
<td>X</td>
</tr>
<tr>
<td>Create an access control roles</td>
<td>mkaccfg</td>
<td>X</td>
</tr>
<tr>
<td>Task</td>
<td>Associated command</td>
<td>Roles</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Display a user’s access control resource instances</td>
<td>lshmcusr</td>
<td>super administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Display a user’s access control roles</td>
<td>lshmcusr</td>
<td>X</td>
</tr>
<tr>
<td>Display a user’s properties</td>
<td>lshmcusr</td>
<td>X</td>
</tr>
<tr>
<td>Modify a user’s access control resource instances</td>
<td>chhmcusr</td>
<td>X</td>
</tr>
<tr>
<td>Modify a user’s access control roles</td>
<td>chhmcusr</td>
<td>X</td>
</tr>
<tr>
<td>Modify a user’s properties</td>
<td>chhmcusr</td>
<td>X</td>
</tr>
<tr>
<td>Modify an access control role</td>
<td>chaccfg</td>
<td>X</td>
</tr>
<tr>
<td>Remove an access control role</td>
<td>rmaccfg</td>
<td>X</td>
</tr>
<tr>
<td>Remove inactive access control resource instances assigned to a user</td>
<td>rmaccfg</td>
<td>X</td>
</tr>
<tr>
<td>Remove a user from the HMC</td>
<td>rmhmcusr</td>
<td>X</td>
</tr>
<tr>
<td>View an access control resource instance</td>
<td>lsaccfg</td>
<td>X</td>
</tr>
<tr>
<td>View an access control role</td>
<td>lsaccfg</td>
<td>X</td>
</tr>
</tbody>
</table>
Predefined passwords for hscroot and root user IDs

Predefined user IDs and passwords are included with the HMC. It is imperative to your system’s security that you change all predefined passwords immediately.

The following predefined user IDs and passwords are included with the HMC:

<table>
<thead>
<tr>
<th>User ID</th>
<th>Password</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>hscroot</td>
<td>abc123</td>
<td>The hscroot user ID and password are used to log in to the HMC for the first time. They are case-sensitive and can only be used by a member of the super administrator role.</td>
</tr>
<tr>
<td>root</td>
<td>passw0rd</td>
<td>The root user ID and password are used by the service provider to perform maintenance procedures. They cannot be used to log in to the HMC.</td>
</tr>
</tbody>
</table>

HMC network connections

This section describes the different types of network connections you can use to connect your HMC to managed systems.

For more information about configuring the HMC to connect to a network, see “Configuring the HMC using the HMC configuration checklist” on page 58.

For more information about using the HMC on a network, see the following:

- “Types of HMC network connections”
  Describes how to utilize HMC remote management and service functions using your network.

- “Private and open networks in the HMC environment” on page 15
  Explains how a private and open network are used in relation to the HMC.

- “The HMC as a DHCP server” on page 19
  Explains the basics of DHCP and how to use the HMC as a DHCP server.

Types of HMC network connections

The HMC supports the following types of logical communications:

- **HMC to managed system**: This type of communications is used to perform most of the hardware management functions, in which HMC issues control function requests through the service processor of the managed system.

- **HMC to logical partition**: This type of communications is used to collect platform-related information (hardware error events, hardware inventory) from the operating systems running in the logical partitions, as well as to coordinate certain platform activities (dynamic LPAR, concurrent repair) with those operating systems. If you want to use service and error notification features, it is important that you make this connection.

- **HMC to remote users**: This type of communications provides remote users with access to HMC functionality. Remote users can access the HMC in the following ways:
  - By using the remote client to access all the HMC GUI functions remotely
  - By using SSH to access the HMC command line functions remotely
  - By using a virtual terminal server for remote access to virtual logical partition consoles

- **HMC to service provider**: This type of communications is used to transmit data, such as hardware error reports, inventory data, and microcode updates, to and from your service provider. You can use this communications path to make automatic service calls.
The HMC supports up to three separate physical Ethernet interfaces. In the desktop version of the HMC, this consists of one integrated Ethernet and up to two plug-in adapters. In the rack-mounted version, this consists of two integrated Ethernet adapters and up to one plug-in adapter. Use each of these interfaces in the following ways:

- One network interface can be used exclusively for HMC-to-managed system communications, which means that only the HMC and service processors of the managed systems would be on that network. Even though the network interfaces into the service processors are SSL-encrypted and password-protected, having a separate dedicated network can provide a higher level of security for these interfaces.

- Another network interface would typically be used for the network connection between the HMC and the logical partitions on the managed systems, for the HMC-to-logical partition communications. For more information about configuring the HMC to connect to a network, see "Configuring the HMC using the HMC configuration checklist" on page 58. For more information about the communications options you have for logical partitions, see "Communications options for logical partitions".

- The third interface is an optional additional Ethernet connection that can be used for remote management of the HMC. This third interface can also be used to have a separate HMC connection to different groups of logical partitions. For example, you might want to have an administrative LAN that is separate from the LAN on which all the usual business transactions are running. Remote administrators could access HMCs and other managed units using this method. Sometimes the logical partitions are in different network security domains, perhaps behind a firewall, and you might want to have different HMC network connections into each of those two domains.

For more information about physically cabling the HMC to the managed system, see "Cabling your server".

**Private and open networks in the HMC environment**

This topic describes when you might want to use a private network, and when you might want to use an open network.

**Note:** If you are connecting the HMC to the model 9118-575 server or the 590 or 0595 managed servers, you must configure the HMC in a private DHCP network.

The connection between the HMC and its managed systems can be implemented either as a private or open network. The term open refers to any general, public network that contains elements other than HMCs and service processors that is not isolated behind an HMC. The other network connections on the HMC are considered open, which means that they are configured in a way that you would expect when attaching any standard network device to an open network.

In a private service network, however, the only elements on the physical network are the HMC and the service processors of the managed systems. In addition, the HMC provides Dynamic Host Configuration Protocol (DHCP) services on that network, which allow it to automatically discover and assign IP configuration parameters to those service processors. You can configure the HMC to select one of several different address ranges to use for this DHCP service, so that the addresses provided to the service processors do not conflict with addresses used on the other networks to which the HMC is connected. The DHCP services allow the elements on the private service network to be automatically configured and detected by the HMC, while at the same time preventing address conflicts on the network.

On a private network, therefore, all of the elements are controlled and managed by the HMC. The HMC also acts as a functional firewall, isolating that private network from any of the open networks to which the HMC is also attached. The HMC does not allow any IP forwarding; clients on one network interface of the HMC cannot directly access elements on any other network interface.

It is recommended that you implement service network communications through a private network, because of the additional security and ease of setup that it provides. However, in some environments, this is not feasible because of physical wiring, floor planning, or control center considerations. In this
case, the service network communications can be implemented through an open network. The same functionality is available on both types of networks, although the initial setup and configuration on an open network require more manual steps.

The following figures show various representations of private and open networks:

Figure 2. Private network: direct connection
Figure 3. Private network: indirect connection
Choosing a private network

Designate the first HMC network interface as private if any of the following is true:

- Only the HMC and service processors will be endpoints on that network.
- All elements will be connected in a single subnet, and you will not be routing or switching.
- You want the HMC to automatically configure and detect the managed systems associated with those service processors.
- You want to keep the service network isolated “behind” the HMC.
Choosing an open network

Designate the first network interface as open if you want to run the communications between the HMC and the service processors across an open network that crosses multiple subnets or has other devices on the network.

For more information about choosing a network type, see “Selecting the network type” on page 60.

The HMC as a DHCP server

If you want to configure the first network interface as a private network, you will have the option of selecting from a range of IP addresses for the DHCP server to assign to its clients. The selectable address ranges include segments from the standard nonroutable IP address ranges.

In addition to these standard ranges, there is also a special range of IP addresses that is reserved for this use. This special range can be used to avoid conflicts in cases where the HMC-attached open networks are using one of the nonroutable address ranges. Based on the range selected, the HMC network interface on the private network will be automatically assigned the first IP address of that range, and the service processors will then be assigned addresses from the rest of the range.

The DHCP server in the HMC uses automatic allocation, which means that each unique service processor Ethernet interface will be reassigned exactly the same IP address each time it is started. Each Ethernet interface has a unique identifier based upon a built-in Media Access Control (MAC) address, which allows the DHCP server to reassign the same IP parameters.

Figure 5. Private network with one HMC as a DHCP server
For more information about how to configure the HMC as a DHCP server, see “Configuring the HMC as a DHCP server” on page 61.

Web-based System Manager Remote client

This is the topic sentence of my kick-off article or parent article. (I may also use this template as a high-level or low-level parent article.)

I’ll include one or two paragraphs that introduce this kick-off (or parent) article. (If the information is so much that I need a list or need too many paragraphs, I’ll use an inline link to this background and prerequisite information.)

Links to children (Do not use a subheading here unless you have groups of links to children.)

Here is my introduction to this list of user tasks. (The order and number of children links in the nav bar should match the order and number of children links in my kick-off or parent article.)

“Installation requirements for the remote client”
Ensure that your PC is compatible with the remote client.

“Remote client comparison”
Determine whether to install the Web-based System Manager Remote Client or the Web-based System Manager Remote Client for Java Web Start on your PC.

“System Manager Security” on page 21
Understand how to secure the HMCs in your environment.

Installation requirements for the remote client

To install the remote client on a PC, your computer must meet the following requirements:

- Either Microsoft® Windows® (supported versions include Windows 2000, Windows XP, and Windows Server 2003) or the Linux operating systems (supported versions include Red Hat Enterprise Linux Version 3, SUSE LINUX Enterprise Server (SLES) 8, SLES9, and SUSE LINUX version 9.0 and 9.1)
- 150 MB of free disk space on the default drive for temporary use during the installation procedure
- 150 MB of free disk space on the drive that you plan to use to install the remote client
- Minimum PC processor speed of 1 GHz
- Minimum of 512 MB of memory (1 GB of memory is recommended for better performance)

Remote client comparison

You can access your HMC remotely by installing the Web-based System Manager remote client on your PC. The remote client provides great flexibility by allowing you to manage your system from virtually anywhere you have a PC. There are two types of remote clients you can install, the Web-based System Manager Remote Client and the Web-based System Manager Remote Client for Java Web Start. After you launch the remote client, there is no difference between the two.
The following table lists the similarities and differences between the remote clients:

<table>
<thead>
<tr>
<th>Web-based System Manager Remote Client for Java Web Start</th>
<th>Web-based System Manager Remote Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Available for Linux and Windows platforms</td>
<td>• Available for Linux and Windows platforms</td>
</tr>
<tr>
<td>• Checks for updates every time it launches and if updates are available, downloads them automatically</td>
<td>• Updates require that you uninstall the previous version and install the current version</td>
</tr>
<tr>
<td>• Launches from the Java Web Start console</td>
<td>• Installs via an InstallShield wizard</td>
</tr>
<tr>
<td>• Automatic update downloads may impact performance if you are using a cable modem or DSL connection</td>
<td>• You can select the installation location</td>
</tr>
<tr>
<td>• Requires an HTTP server</td>
<td></td>
</tr>
</tbody>
</table>

System Manager Security

System Manager Security ensures that the HMC can operate securely in client/server mode. Servers and clients communicate over the Secure Sockets Layer (SSL) protocol, which provides server authentication, data encryption, and data integrity. Each System Manager server has its own private key and a certificate of its public key signed by a certificate authority (CA) that is trusted by the System Manager clients. The private key and the server certificate are stored in the server’s private key ring file. Each client must have a public key that contains the certificate of the trusted CA.

A Certificate Authority (CA) is a trusted central administrative entity (a local HMC in this situation) that can issue digital certificates to clients and servers (HMC4 in Figure 6 on page 22). The trust in the CA is the foundation of trust in the certificate as a valid credential. A CA uses its private key to create a digital signature on the certificate that it issues to validate the certificate’s origin. Others, such as System Manager clients, can use the CA certificate’s public key to verify the authenticity of the certificates that the CA issues and signs.

Every digital certificate has a pair of associated cryptographic keys. This pair of keys consists of a public key and a private key. A public key is part of the owner’s digital certificate and is available for anyone to use. A private key, however, is protected by and available only to the owner of the key. This limited access ensures that communications that use the key are kept secure. The owner of a certificate can use these keys to take advantage of the cryptographic security features that the keys provide. For example, the certificate owner can use a certificate’s private key to "sign" and encrypt data sent between clients and servers, such as messages, documents, and code objects. The recipient of the signed object can then use the public key contained in the signer’s certificate to decrypt the signature. Such digital signatures ensure the reliability of an object’s origin and provide a means of checking the integrity of the object.

A server is an HMC you want to access remotely. In Figure 6 on page 22, HMCs 1, 3, and 4 are servers. A client is a system from which you want to access other HMCs remotely. In Figure 6 on page 22, Web-based System Manager Remote Clients A, B, and C, and HMCs 1, 2, and 5 are clients. As shown in Figure 6 on page 22, you can configure multiple servers and clients in your private and open networks.

An HMC can be multiple roles simultaneously. For example, an HMC can be a client and a server like HMC1 in Figure 6 on page 22. An HMC can also be a CA, server, and client at the same time.
Each server must have a unique private key and a certificate of its public key signed by a CA that is trusted by the clients. Each client must have a copy of the CA’s public key.

The following is an overview of tasks involved in Chapter 5, “Installing and securing the remote client,” on page 65
1. Configure one HMC as a Certificate Authority (CA).
2. Use this HMC to generate private keys for the servers.
3. Install the private keys on the servers.
4. Configure the servers as secure System Manager servers.
5. Distribute the CA’s public key to the servers or clients.

Note: Tasks 3 and 5 are completed by copying the keys to diskette and installing them on the servers or clients.
Chapter 4. Setting up the HMC

To set up the Hardware Management Console (HMC), you must complete three main groups of tasks: cabling the HMC to the managed server, gathering configuration settings for your installation, and configuring the HMC. The HMC can be a stand-alone HMC or an HMC you plan to install in a rack. Use the topics below to complete these tasks.

If you are setting up the HMC in conjunction with the setup of a new server, you must perform these tasks in conjunction with other tasks related to your server setup. See Initial server setup for detailed instructions.

"Cabling the HMC" on page 26
Connect the HMC cables, connect the Ethernet cable, and connect the HMC to power.

"Gathering required configuration settings" on page 48
Use the table provided in this topic to gather required configuration settings that you need to know before you begin the configuration steps.

"Configuring the HMC" on page 53
Configure network connections, security, service applications, and some user preferences.

Note: Once you have completed the HMC setup, do not power down or disconnect the HMC from the managed system. If the HMC is powered down or disconnected from a nonpartitioned managed system for a period of 14 days, the managed system will no longer recognize the HMC. If this situation occurs and the managed system fails to recognize the HMC, return to this topic and set up the HMC again.

If your system is partitioned, the 14-day time limit does not apply. Steps for configuring logical partitions are in the "Postconfiguration steps for the HMC" on page 64 topic and can be completed after your HMC is set up.
# Cabling the HMC

**DANGER**

Electrical voltage and current from power, telephone, and communication cables are hazardous.

To avoid a shock hazard:
- Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.
- Connect all power cords to a properly wired and grounded electrical outlet. Ensure outlet supplies proper voltage and phase rotation according to the system rating plate.
- Connect any equipment that will be attached to this product to properly wired outlets.
- When possible, use one hand only to connect or disconnect signal cables.
- Never turn on any equipment when there is evidence of fire, water, or structural damage.
- Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.
- Connect and disconnect cables as described below when installing, moving, or opening covers on this product or attached devices.

To Disconnect:
1. Turn everything OFF (unless instructed otherwise).
2. Remove power cords from the outlet.
3. Remove signal cables from connectors.
4. Remove all cables from devices.

To Connect:
1. Turn everything OFF (unless instructed otherwise)
2. Attach all cables to devices.
3. Attach signal cables to connectors.
4. Attach power cords to outlet.
5. Turn device ON.

(D005)

Use the following instructions to help you cable your rack-mounted or stand-alone HMC.

**Attention:** *Do not* plug the power cords into the electrical outlet until you are instructed to do so.

1. Use the Specifications for HMC to help you ensure that you position the HMC in a proper location.
2. If you are installing a rack-mounted HMC, perform the following steps:
   a. Use the following illustrations to identify the location of the connectors described in these instructions:
b. **Install the HMC into a rack.**

c. **Connect the monitor, keyboard, and mouse:**

   If you are using a rack-mounted LCD monitor and keyboard (model 7316-TF3):
• For connection to a model 7310-CR2 HMC, connect the keyboard and display to the C2T-to-KVM (keyboard, video, mouse) adapter breakout cable that you have previously attached to the HMC. The mouse is integrated with the keyboard.

If you are using a stand-alone monitor, keyboard, and mouse:

• For connection to a model 7310-CR2 HMC, connect the keyboard and display to the C2T-to-KVM (keyboard, video, mouse) adapter breakout cable that you have previously attached to the HMC. If your keyboard and mouse use USB connections, you can also connect them to the USB ports on the front panel of the HMC.

• For connection to a model 7310-CR3 HMC, connect the keyboard, display, and mouse using the USB conversion option cable.

d. Continue with step 4 on page 31

3. If you are installing a stand-alone HMC, perform the following steps:
   a. Use the following illustrations to identify the location of the connectors described in these instructions:
Figure 9. Back view of a stand-alone HMC (7310-C04)

1. PCI connectors (slot 1 to left)
2. PCI Express (x1) connector
3. PCI Express (x16) graphics connector
4. Ethernet connector
5. USB connectors
6. Mouse connector
7. Parallel connector
8. Serial connector (some models)
9. Diagnostic LEDs
10. Power connector
11. Audio line out connector
12. Audio line in connector
13. VGA monitor connector
14. Serial connector
15. Keyboard connector
16. USB connectors
Figure 10. Back view of a stand-alone HMC (7310-C03)

1. Power connector
2. Mouse connector
3. Parallel connector
4. USB connectors
5. Ethernet connector
6. Audio line in connector
7. PCI slots (slot 1 to right)
8. AGP slot
9. Audio line out connector
10. Microphone connector
11. USB connectors
12. VGA monitor connector
13. Serial connector
14. Keyboard connector

b. Attach the monitor cable to the monitor connector, and tighten the screws.
c. Attach the power cord to the monitor.
d. Ensure that the voltage selection switch on the HMC is set to the voltage used in your geography. The voltage selection switch is red and is located near the power connector. Move the switch so that the voltage used in your geography is displayed.

e. Plug the power cord into the HMC.

f. Connect the keyboard and mouse:

**USB connections:** Connect the keyboard and mouse to Universal Serial Bus (USB) ports on the HMC. You can connect the keyboard and mouse to the USB ports on the front or back panels.

**Note:** If you are using a stand-alone model 7310-C01 or 7310-C02 HMC, connect the keyboard and mouse to the front-panel USB ports only.

**PS/2-type connections:** Connect the mouse and keyboard to their connectors on the back panel of the HMC.

g. Continue with step 4

4. Connect the modem:

**Note:** During the installation and configuration of the HMC, the modem might automatically dial out as the HMC follows routine call-out procedures. This is normal behavior.

*If you are connecting an external modem:*

a. Optional: Install the external modem into a rack

b. If you have not already done so, connect the modem data cable to the external HMC modem.

c. Connect the modem data cable to the serial port on the HMC labelled with the following symbol:

![Symbol]

**Note:** If you are connecting to an integrated modem, use the data cable to connect the integrated HMC modem to the appropriate data source. For example, use the telephone cable to connect the HMC modem **LINE** port to the analog jack on your wall.

5. Connect the Ethernet (or crossover) cable from the HMC to the managed server:

**Notes:**

a. In general, your HMC should be connected to the managed server in a private service DHCP network; specifically, your HMC connection to the 9118-575 server and the 590 and 595 servers **must** be made in a private service DHCP network. This requires that you use the Ethernet port that is defined as eth0 on your HMC.

   • If you have not installed any additional Ethernet adapters in the PCI slots on your HMC, use the primary integrated Ethernet port to complete the following instructions. Refer to the illustrations to see the location of these ports.

   • If you have installed additional Ethernet adapters in the PCI slots, see "Identifying the Ethernet port defined as eth0" on page 47 to determine which Ethernet port you must use.

b. You can verify that the Ethernet cable connection is active by observing the green status lights at both the HMC and managed system Ethernet ports as your installation progresses.
Connect the Ethernet port on the HMC to the Ethernet port that is labeled HMC1 on the managed server. On the model 9118-575 server and the 590 and 595 servers, use the port labelled J00A on the front bulk power control assembly.

If you are connecting a second HMC to your managed server, connect to the Ethernet port that is labeled HMC2 on the managed server; on the 9118-575 server and the 590 and 595 servers, use the port labelled J00A on the rear bulk power control assembly.

6. If you use an external modem, plug the modem power supply cord into the HMC modem.
7. Plug the power cords for the monitor, HMC, and HMC external modem into electrical outlets.

**Note:** Do not connect the managed system to a power source.

8. If you are setting up the HMC to manage a new server, go to Cabling your server Click Select by model and choose the model server you want to cable, then select the console you are using, and complete the remaining steps in that checklist.
9. If you are setting up the HMC to manage an existing server, continue with “Gathering required configuration settings” on page 48.

**Installing the HMC into a rack**
The following steps are required to install the HMC into a rack:

**Note:** Blue on a part of the hardware indicates a touch point where you can grip the hardware to remove it from or install it in the managed system, open or close a latch, and so on.

**DANGER**

- Always lower the leveling pads on the rack cabinet.
- Always install stabilizer brackets on the rack cabinet.
- To avoid hazardous conditions due to uneven mechanical loading, always install the heaviest devices in the bottom of the rack cabinet. Always install servers and optional devices starting from the bottom of the rack cabinet.
- Rack-mounted devices are not to be used as a shelf or work space. Do not place any object on top of rack-mounted devices.
- Each rack cabinet might have more than one power cord. Be sure to disconnect all power cords in the rack cabinet before servicing any device in the rack cabinet.
- Connect all devices installed in a rack cabinet to power devices installed in the same rack cabinet. Do not plug a power cord from a device installed in one rack cabinet into a power device installed in a different rack cabinet.
- An electrical outlet that is not correctly wired could place hazardous voltage on the metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock.
CAUTION:

- Do not install a unit in a rack where the internal rack ambient temperatures will exceed the manufacturer’s recommended ambient temperature for all your rack-mounted devices.
- Do not install a unit in a rack where the air flow is compromised. Ensure that air flow is not blocked or reduced on any side, front, or back of a unit used for air flow through the unit.
- Consideration should be given to the connection of the equipment to the supply circuit so that overloading of the circuits does not compromise the supply wiring or overcurrent protection. To provide the correct power connection to a rack, refer to the rating labels located on the equipment in the rack to determine the total power requirement of the supply circuit.
- *(For sliding drawers.)* Do not pull out or install any drawer or feature if the rack stabilizer brackets are not attached to the rack. Do not pull out more than one drawer at a time. The rack may become unstable if you pull out more than one drawer at a time.
- *(For fixed drawers.)* This drawer is a fixed drawer and should not be moved for servicing unless specified by manufacturer. Attempting to move the drawer partially or completely out of the rack may cause the rack to become unstable or cause the drawer to fall out of the rack.

(R001)

1. Use the following illustration to ensure that you have all the items that you need to install the HMC in your rack enclosure. If any items are missing or damaged, contact your place of purchase. For further information about the rack hardware, refer to the documentation that was provided with the rack enclosure.

Attention:  Do not place any object weighing more than 50 kg (110 lbs) on top of devices mounted on the rack.
2. Starting with the slide rail that is marked **LEFT/FRONT**, complete the following tasks to prepare the slide rail for installation in the rack.
   a. To prevent the rail-adjustment bracket from moving during the next step, press and hold the back of the rail-adjustment bracket 3.
   b. On the back end of the rail, while holding the blue tab 1 open, press the blue tab 2 to slide the back rail-locking carrier toward the front end until it clicks into the open position.
   c. On the front end of the rail, while holding the blue tab 1 open, press the blue tab 2 to slide the front rail-locking carrier toward the back end until it clicks into the open position.
3. Position the rail so that the pins on the back rail-locking carrier align with the holes on the back rail-mounting flange. Press the blue tab 1 to release the rail-locking carrier and secure the back of the slide rail onto the back rack-mounting flange.

**Attention:** Ensure that the pins are fully extended through the mounting flange and slide rail 2.

If you need to adjust the slide-rail length, lift the tab 3 and extend the rail-adjustment bracket from the back of the slide rail until it is the appropriate length.
4. Making sure that the rail is level, align the pins 3 on the front rail-locking carrier to the front rack-mounting flange 2. If you adjusted the rail length, push the front rail flange back.
Press the blue tab 1 to release the rail-locking carrier and secure the front of the slide rail onto the front rack-mounting flange.

Attention: Ensure that the pins 3 are fully extended through the mounting flange and the slide rail 4.

5. Repeat steps 1 through 4 for the slide rail marked RIGHT/FRONT.
6. Align the HMC on the slide rails and push the HMC fully into the rack enclosure. Secure the HMC to the front mounting flanges with the two thumbscrews 1.
7. If the shipping brackets impede the HMC from fully setting into the rack enclosure, remove them by pressing on the tab 1 as indicated on the shipping bracket, and slide the shipping bracket off the slide rail. Repeat this step for the other shipping bracket. Store the shipping bracket for future use.

![Diagram 1](IPHA505-0)

**Note:** You must reinstall the shipping brackets on the slide rails before you transport the rack enclosure to another location with the HMC installed. To reinstall the shipping bracket, reverse this step.

8. If you are installing a 7310-CR2 HMC, connect the breakout cable (the C2T-to-KVM adapter cable for the keyboard, monitor, and mouse that comes with your HMC) to the port labeled OUT on the back of the HMC, and connect the power cable to the back of the HMC. If you are installing a 7310-CR3 HMC, connect the USB conversion option cable to a USB connector. Route the cables to the lower-left corner of the HMC (as viewed from the back), and use the cable straps 1 to secure the cables to the slide rails.

![Diagram 2](IPHA506-0)
9. If you plan to transport the rack enclosure to another location with the HMC installed, complete the following tasks to secure the HMC to the rack:

Note: To remove the HMC from the rack, reverse these instructions.

a. Disconnect the cables from the back of the HMC.

b. Slide the HMC out of the rack about 150 mm (6 inches), and insert the M6 screws in the front of each slide rail 2.

c. At the back of the rack secure the HMC to the rack enclosure with M6 screws 1 and reconnect the cables.

d. Reinstall the shipping brackets on the slide rails. To reinstall the shipping brackets, reverse the procedure in step 6 on page 37.

e. Push the HMC back into the rack and secure it to the rack using the thumbscrews on the front of the rack.

f. Reconnect any cables that were disconnected.

10. Continue with step 2c on page 27.

Installing the external modem into a rack

The modem tray supports the MultiTech Systems MultiModem II Model MT5600BA Series modem. The modem tray attaches to the system rack and holds one or two standalone modems, gateways, or other networking equipment. The modem tray occupies 1 Electronics Industries Association (EIA) location in the rack. If only one modem or other networking unit is installed in the modem tray, a blank filler is used in the empty mounting location to ensure that proper airflow is maintained in the rack. The blank filler also ensures that electromagnetic interference is confined within the rack.

Check the power source on the rack

Ensure that the correct power source is available on the rack. The MultiTech Systems MultiModem II Model MT5600BA Series modems are equipped to operate on 120 V ac, 60 Hz, 16 W, or 230 V / 50 Hz (international). Racks have power distribution buses (PDB) 2 that supply the correct alternating current.
and power to operate the modems installed in the modem tray. The PDBs are located at the back and bottom of the rack as shown in the following illustration:

![Diagram showing the location of PDBs and the modem tray.]

**Note:** The main power source plug on the rack is indicated by 1.

**Install the modem into the modem tray**

1. Remove the screw 5 securing the retaining bracket 6 at the back of the modem tray 4. The retaining bracket can now be removed from the modem tray. See the following illustration.

2. Position the modem in the tray 4 or 7 with the front of the modem facing the front of the tray. Slide the front of the modem under the two retainer tabs 3.
3. Position the retaining bracket that was removed in step 1 over the back corner of the modem.
4. Align the screw hole in the retaining bracket to the hole at the back of the modem tray.
5. Reattach the retaining bracket to the back of the modem tray by tightening the retaining bracket screw. The installed modems are shown in the following illustration:

6. Are you installing a second modem?
   Yes:
   a. Loosen the two screws in the blank filler to detach the filler from the modem tray.
   b. Remove the blank filler from the front of the empty mounting location. See the following illustration.
   c. Repeat steps on page through to install a second modem.
   No: Continue with the next step.

**Install the modem tray into the rack**
1. Open the rack front and back doors.
2. Determine the EIA location for mounting the modem tray into the rack. The modem tray must be mounted at an EIA location adjacent to a horizontal cable-routing support rail on the rack. This mounting location enables the modem data cables and power cables to be properly routed and secured. The horizontal cable-routing support rails can be identified by their pattern of holes along the rails. The following illustration shows the top horizontal, middle horizontal, and bottom horizontal cable routing support rails. It then indicates suitable locations for the modem tray.
3. Install nut clips 1 on each of the front vertical rails of the rack at the selected EIA installation location 2 as shown in the following illustration.

4. Position the modem tray at the selected installation location, and slide the modem tray into the rack. Ensure that the mounting screw holes on the modem tray align with the nut clips installed on the rack front vertical rails.

5. Insert and tighten the mounting screws.

6. Connect the data cables to the modem by completing the following steps:

   **Note:** For detailed information about data cable connections, refer to the documentation from the modem manufacturer.

   a. Attach the RS232 cable to the back of the modem. The RS232 cable’s pin configuration can be 25-pin to 25-pin, or 9-pin to 25-pin.

   b. Determine the type of additional data cables that will be attached. The modem can operate with either of the following cables:
• Leased line. Pin configuration can be two-wire or four-wire.
• Telephone line.

c. Attach the data cables to the back of the modem. Ensure that the pin configuration described in the modem manufacturer’s documentation is followed.

**Note:** To gain adequate access to the back of the modem, it might be necessary to slide the system drawer that is located above or below the modem tray out of the rack.

7. Peel off the adhesive covering located on the bottom of each cable clamp. Position two cable clamps to each side of the modem tray as shown in the following illustration. Press firmly to adhere the cable clamps to the modem tray. The cable clamps will be used to route cables to the horizontal rack rail.

8. Connect the modem power supply cord to the power connector located on the back of the modem.

9. To avoid cables and the power cord getting pinched between units, route the cables and power cord through the cable clamps located on the side of the modem tray.

10. Route the power cord and data cables from the modem to the appropriate horizontal rail adjacent to the modem tray installation location on the rack.

**Note:** Route the cables and cord to the closest horizontal support rail. To avoid damage to the cables when other units are slid in or out, ensure the cables and cord are routed within the EIA space for the modem tray.

The horizontal support rails are located on both sides of the rack. The following illustration shows the bottom, middle, and top horizontal support rails. It also shows an example of a cable and cord route at the top of the rack and on the horizontal rails.
11. Secure the power cord and data cables 3 to the horizontal rail using the hook-and-loop cable ties 2. See the following illustration for more detail.
Note: The modem is indicated by 1 and the cable clamps are indicated by 4.

Note: Before securing the cables and cord, ensure that the connector on each cable or cord is accessible to its destination (such as the data cable reaching the HMC and the power cord from the power supply reaching the PDB).

12. Attach one strip of double-sided adhesive to the bottom of the power supply.

Note: The bottom of the power supply is the clear surface located opposite the side with the label attached.

13. Position the power supply at the mounting location on the inside of the rack side panel, and press it firmly to adhere the power supply to the rack.

14. Attach a strip of hook-and-loop cable ties to the back vertical rail of the rack.

15. Route the power cord from the power supply to the PDB located at the back of the rack.

Note: Do not connect the power during this step.

Complete the installation
1. Connect the power cord from the modem to the PDB 2 located inside and at the back of the rack.

See the following illustration for the location of the PDB.
Note: The main power source plug on the rack is indicated by \[ \text{Figure 1} \].

2. Connect the modem to an HMC:
   • If you are connecting the modem to an HMC installed in a rack, plug the RS232 cable into the serial port located below the following symbol:

   ![Symbol](image1.png)

   • If you are connecting the RS232 data cable to a stand-alone HMC, plug the cable into serial port 2 (S2). Serial port 2 is the 9-Pin D-Shell socket noted by either of the following symbols:

   ![Symbol](image2.png)
3. If you are connecting the RS232 data cable to equipment other than an HMC, follow the equipment manufacturer’s instructions for connecting the cables.

4. Close the rack front and back doors.

5. Continue with step 4b on page 31.

**Identifying the Ethernet port defined as eth0**

Your Ethernet connection to the managed server must be made using the Ethernet port that is defined as eth0 on your HMC.

If you have not installed any additional Ethernet adapters in the PCI slots on your HMC, the primary integrated Ethernet port is always defined as eth0.

If you have installed additional Ethernet adapters in the PCI slots, the port that is defined as eth0 depends on the location and type of Ethernet adapters you have installed:

<table>
<thead>
<tr>
<th>HMC type</th>
<th>Rules for Ethernet placement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rack-mounted HMC</td>
<td>The HMC supports only one additional Ethernet adapter card.</td>
</tr>
<tr>
<td></td>
<td>• If an additional Ethernet adapter is installed, that port is defined as eth0. In this case,</td>
</tr>
<tr>
<td></td>
<td>the primary integrated Ethernet port is then defined as eth1, and the secondary integrated</td>
</tr>
<tr>
<td></td>
<td>Ethernet port is defined as eth2.</td>
</tr>
<tr>
<td></td>
<td>• If no adapter cards are installed, the primary integrated Ethernet port is defined as eth0.</td>
</tr>
<tr>
<td>Stand-alone model 7310-C04 HMC</td>
<td>The definitions depend upon the type of Ethernet adapter card or cards you have installed:</td>
</tr>
<tr>
<td></td>
<td>• If only one Ethernet adapter card is installed, whether it is a 1 Gigabit Ethernet adapter</td>
</tr>
<tr>
<td></td>
<td>or a 10/100 Ethernet adapter, that adapter is defined as eth0.</td>
</tr>
<tr>
<td></td>
<td>• If both a 10/100 Ethernet adapter and a 1 Gigabit Ethernet adapter are installed, the 1</td>
</tr>
<tr>
<td></td>
<td>gigabit adapter is always defined as eth0.</td>
</tr>
<tr>
<td></td>
<td>• If two 10/100 Ethernet adapters are installed, the adapter in slot 1 is defined as eth0.</td>
</tr>
</tbody>
</table>
|                                       | • If two 1 Gigabit Ethernet adapters are installed, the adapter in slot 1 is defined as eth0.
<table>
<thead>
<tr>
<th>HMC type</th>
<th>Rules for Ethernet placement</th>
</tr>
</thead>
</table>
| Stand-alone model 7310-C03 HMC | The definitions are dependent upon the type of Ethernet adapter card or cards you have installed:  
  - The 1 Gigabit Ethernet adapter card, when present, is generally defined as the eth0 location. The exception to this rule is when it is placed in slot 1 (the rightmost PCI slot when viewing the HMC from the rear); however, this placement is not recommended.  
  - If multiple 1 Gigabit Ethernet adapter cards are installed, the configuration is defined in the following order: slot 2 is eth0, slot 3 is eth1, and the integrated Ethernet port is eth2.  
  - If adapter cards other than the 1 Gigabit Ethernet adapter are installed, the integrated Ethernet port is always defined as eth0. |

### Gathering required configuration settings

To successfully configure the HMC, you must understand related concepts, make decisions, and prepare information. Use the following table to identify and gather the information you will need when you configure the HMC.

When you have completed this preparation step, go to [“Configuring the HMC” on page 53](#).

This topic describes planning information for how you want to connect your HMC to your server, to your company network, and to your service provider. Review the related information in the following table to learn more about the decisions you need to make. You might choose to print this page to write down your decisions, requirements, and settings for easy access during the configuration steps.

This information contains references to tasks that are not included in this PDF. You can access the IBM eServer Hardware Information Center on the HMC or on the Web. On the HMC, the information center is in the **Information Center and Setup Wizard** folder. On the Web, the information center is at [http://www.ibm.com/server/library/infocenter](http://www.ibm.com/server/library/infocenter). Select your geographical location, your language preference, and **eServer hardware**.

#### Table 1. Preparing for configuration

<table>
<thead>
<tr>
<th>Preparation topic</th>
<th>Where to find related information</th>
</tr>
</thead>
</table>
| Optional: If you plan to create additional users, identify the following information:  
  - How many user IDs you want to create  
  - The user ID and password for each additional user you plan to create  
  - What role you plan to assign each user | Overview of roles |
| Determine whether you want to specify the media speed for each Ethernet adapter or let the HMC automatically detect the speed.  
  For initial setup, automatic detection is recommended. However, in some situations, you might want to reduce the speed of the adapter. If you plan to specify the media speed for each Ethernet adapter, identify the media speed and duplex mode for each Ethernet adapter. For example, 100 Mbps full duplex. |
### Table 1. Preparing for configuration (continued)

<table>
<thead>
<tr>
<th>Preparation topic</th>
<th>Where to find related information</th>
</tr>
</thead>
</table>
| Prepare the following contact information:  
  • Company name  
  • Administrator’s name  
  • E-mail address  
  • Telephone numbers  
  • Fax numbers  
  • Street address and telephone number for the location of the HMC | |
| Determine what type of connection you want to configure to contact your service provider:  
  • Dial-up from the local HMC:  
    Determine what telephone numbers you will use to call IBM.  
  • Virtual private network (VPN) through the Internet  
  • Connecting through other systems or partitions:  
    Determine the IP addresses or host names of the systems or logical partitions that the HMC passes through when connecting to your service provider. | Choosing your connection method to your service provider |
| Determine whether to register for IBM Electronic Service Agent™. If you decide to register, complete the following tasks:  
  1. Go to [My IBM Profile](#), click Register, and follow the registration instructions.  
  2. Record your two IBM registered IDs if you plan to authorize users to the Electronic Service Agent information. | Electronic Service Agent |
| Identify the Simple Mail Transfer Protocol (SMTP) server and e-mail addresses that should receive notification when problem events occur on the system. | Overview of the managed system passwords |
| Determine the following passwords needed to access the managed system. These will be used later when the managed system is powered on.  
  • Determine the password you want to use to allow the HMC to access the managed system.  
  • Determine the password you want to assign the Advanced System Management (ASM) general user ID.  
  • Determine the password you want to assign to the ASM administrator user ID. | |
| If you plan to add managed systems, identify what systems you plan to add and refer to Figures 3, 4, and 5 to determine how they fit into your network. | |
| Determine whether you plan to connect the HMC to a private or open network.  
A private service network provides greater security and is easier to set up. A private service network allows the HMC to automatically detect the managed system. Therefore, it is recommended that you connect the HMC to a private service network. **Note:** If you are connecting the HMC to the model 9118-575 server or the 590 or 595 managed servers, you must configure the HMC in a private DHCP network. | "Private and open networks in the HMC environment" on page 15 |
Table 1. Preparing for configuration (continued)

<table>
<thead>
<tr>
<th>Preparation topic</th>
<th>Where to find related information</th>
</tr>
</thead>
</table>
| To connect the HMC to a **private service network**, complete the following preparation tasks:  
1. Determine the HMC hostname and domain name. Optionally, you can also enter a phrase in the description field. These settings are used to identify your HMC.  
   **Note:** This step is necessary only if you plan to connect the HMC to an open network after connecting the HMC to a private service network.  
2. Determine whether to configure the HMC as the Dynamic Host Configuration Protocol (DHCP) server. If this is the first or only HMC in your private service network, you must configure the HMC as a DHCP server (see Figure 11 on page 51). If this is an additional local HMC on the private service network, configure it as a DHCP client (see Figure 12 on page 52).  
3. Select one of the following standard nonroutable IP address ranges for your private service network:  
   - 192.168.0.2 – 192.168.255.254  
   - 172.16.0.3 – 172.16.255.254  
   - 172.17.0.3 – 172.17.255.254  
   - 10.0.0.2 – 10.0.0.254  
   - 10.0.128.2 – 10.0.143.254  
   - 10.0.255.2 – 10.0.255.254  
   - 10.1.0.2 – 10.1.15.254  
   - 10.1.255.2 – 10.1.255.254  
   - 10.127.0.2 – 10.127.15.254  
   - 10.127.255.2 – 10.127.255.254  
   - 10.128.0.2 – 10.128.15.254  
   - 10.128.240.2 – 10.128.255.254  
   - 10.254.0.2 – 10.254.0.254  
   - 10.254.240.2 – 10.254.255.254  
   - 10.255.0.2 – 10.255.0.254  
   - 10.255.240.2 – 10.255.255.254  
   - 10.255.143.254  
   - 9.6.24.2 – 9.6.24.254  
   - 9.6.25.2 – 9.6.25.254  
   **Note:** If you decide to connect your private service network to an open network in the future, using standard nonroutable IP addresses now will allow your DHCP servers to co-exist on the open network.  
4. If you plan to configure the HMC as a DHCP client, an IP address is generated by the HMC already in the private service network (see Figure 12 on page 52). If you choose to use static IP addresses, select an address that is within the range used by the other systems in the network. |
| “The HMC as a DHCP server” on page 19 |
| To configure an **open network**, first configure a private service network, and then connect a different adapter on the HMC to your company network. If you plan to connect the HMC to an open network, complete the following preparation tasks:  
1. Complete the preparation tasks for configuring a **private service network** and then continue with the following steps.  
2. Complete the following preparation tasks to connect your private service network to an open network:  
   a. If you plan to enable Domain Name System (DNS), complete the following tasks:  
      1) Identify the DNS server IP addresses.  
      2) Determine the order in which the addresses will be searched.  
      3) Determine the order in which the domain suffixes will be searched.  
   b. Select the adapter to use as the default gateway for the open network.  
   c. Identify the gateway address.  
   d. If you plan to control the HMC remotely or give remote access to others, you must change the firewall settings to the HMC. Identify the applications or IP addresses you want to allow through the HMC’s firewall (see Figure 13 on page 53). |
Figure 11. Private service network: Example 1
Figure 12. Private service network: Example 2
Configuring the HMC

Depending on the level of customization you intend to apply to your HMC configuration, you have several options for setting up your HMC to suit your needs. The Guided Setup wizard is a tool on the HMC designed to make the setup of the HMC quick and easy. You can choose a fast path through the wizard to quickly create the recommended HMC environment, or you can choose to fully explore the

Figure 13. Open network
available settings that the wizard guides you through. You can also perform the configuration steps without the aid of the wizard using the **HMC configuration checklist**

Before you start, you should gather the required configuration information that you will need to complete the steps successfully. See “Gathering required configuration settings” on page 48 for a list of the required information.

**Recommended method:** "**Configuring the HMC using the fast path through the Guided Setup wizard**"

**Recommended:** In most cases, the HMC can be set up to operate effectively using many of the default settings. Use this fast path checklist to prepare the HMC for service quickly and efficiently. When you have completed the steps in this checklist, your HMC will be configured as a Dynamic Host Configuration Protocol (DHCP) server in a private (directly connected) network.

"**Configuring the HMC using the Guided Setup wizard** on page 56

**Custom:** The Guided Setup wizard guides you through numerous configuration settings that you might choose to use in your environment.

"**Configuring the HMC using the HMC configuration checklist**” on page 58

**Custom:** The HMC configuration checklist provides a complete list of all HMC configuration tasks, guiding you through the process of successfully configuring your HMC. Choose this option if you prefer not to use the Guided Setup wizard.

**Configuring the HMC using the fast path through the Guided Setup wizard**

The Guided Setup wizard guides you through a wide range of configuration options that you might need to consider when you set up your HMC. Often, however, the HMC can be set up to operate effectively using many of the default settings. Use this checklist to prepare the HMC for service quickly and efficiently. When you have completed the steps in this checklist, your HMC will be configured as a Dynamic Host Configuration Protocol (DHCP) server in a private (directly connected) network.

**Prerequisites**

To complete the Guided Setup wizard using the fast path, you need to have the following information available:

- New passwords for the predefined **hscroot** and **root** user IDs. These passwords must be at least 7 characters long.
- Details about your company:
  - Administrator name
  - Telephone and fax numbers
- Details about the geographic location of your HMC
- Optional: Your IBM ID for the Electronic Service Agent. You must register at the following Web site to obtain this ID:
  https://www.ibm.com/registration/selfreg
- Optional: SMTP server and e-mail addresses for problem notification.
- New passwords for the managed system, the Advanced System Management general user ID, and the Advanced System Management administrator user ID.

**Start the fast path through the Guided Setup wizard**

Follow these steps to quickly configure your HMC:

**Starting the HMC and setting passwords**
1. Ensure that the managed system is not connected to a power source. For rack-mounted HMCs, this means that the only device plugged into the power distribution bus (PDB) before you plug in the main power supply is the HMC. (See the “Cabling the HMC” on page 26 topic if you are not sure.)

2. Press the power button on the HMC to turn it on.

3. Wait for the HMC to automatically select the default language and locale preference after 30 seconds.

4. Sign in to the HMC:
   - ID: hscroot
   - Password: abc123

5. To continue, accept the Hardware Management Console license agreements. If you decline the Hardware Management Console license agreements, you cannot complete the HMC configuration.

6. Click **OK** on the Guided Setup entry window.

7. Click **Next** on the Welcome window.

8. Verify and change, if necessary, the time, date, and time zone settings. Click **Next**.

9. Change the **hscroot** password:
   a. Enter the new password twice. The password must be at least 7 characters long.
   b. Click **Next**.

10. Change the **root** password:
    a. Enter the new password twice. The password must be at least 7 characters long.
    b. Click **Next**.
    c. Click **Next** again.

11. Click **Next** on the Next Steps summary window.

**Configuring network settings**

1. On the second Configure Network Settings window, select the LAN adapter labeled eth0. Click **Next**.

2. On the LAN adapter speed window, click **Next**.

3. On the Configure (LAN adapter name) window, click **Next**.

4. On the second Configure (LAN adapter name) window, select private service network. Click **Next**.

5. On the third Configure (LAN adapter name) window, select **Yes, enable the HMC as a DHCP server**. Click **Next**.

6. On the Configure Network Settings window, select **No**. (You can configure any remaining LAN adapters later.) Click **Next**.

7. Click **Next** on the Next Steps summary window.

**Configuring connectivity to your service provider**

1. On the Specify Contact Information window, type the contact information for the administrator of your HMC. Click **Next**.

2. On the Specify Contact Information window, type the contact address information for the location of your HMC. Click **Next**.

3. On the Specify Contact Information window, select the **Use the administrator mailing address** box, or clear it to enter a different address for the HMC, as required. Click **Next**.

4. On the Configure Connectivity to Your Service Provider window, click **Next**.

5. Click **Accept** on the Agreement for Service Programs window.

6. On the Configure Dial-up from the Local HMC window:
   a. Click **Modem Configuration**. If you must dial a number to call off-site at your company, type the number in the **Dial prefix** field. Click **OK**.
   b. To add a telephone number to your service provider, click **Add**.
      1) Select the appropriate country or region.
2) Select the appropriate state or province.
3) Select the appropriate telephone number from the list.
4) In the Phone number field, edit the selected telephone number, if necessary. For instance, if the selected telephone number is a local call from your site, you might need to remove the area code.
5) Click OK.

7. On the Authorize Users for Electronic Service Agent window, enter your IBM IDs (skip this step if you do not have an IBM ID). Click Next.
8. On the Notification of Problem Events window, specify the SMTP server and port. Click Add to specify one or more e-mail addresses for notification of problem events. Click Next.

**Monitoring your configuration**

1. On the Status window, monitor the progress of the different configuration settings you selected.
   - This window might show a status of Pending for some tasks for several minutes.
   - Click View Log to see status messages relating to each task. Click OK on the status message window to close it.
   - Click Close at any time to close the Guided Setup wizard. Tasks that are still running will continue to run.

**Configuring the HMC using the Guided Setup wizard**

Use these instructions to perform a customized configuration of your HMC.

**Note:** Use the fast path through the Guided Setup wizard to complete configuration of your HMC quickly and easily with minimal customization. See "Configuring the HMC using the fast path through the Guided Setup wizard" on page 54 for instructions.

**Prerequisites**

Complete the configuration preparation activity described in the "Gathering required configuration settings" topic.

**Run the Guided Setup wizard**

Use the following instructions to configure your HMC using the Guided Setup wizard.

**Note:** If you are connecting the HMC to the model 9118-575 server or the 590 or 595 managed servers, you must configure the HMC in a private DHCP network using the eth0 Ethernet connection.

1. Ensure that the managed system is not connected to a power source.
2. Start the Guided Setup wizard:
   a. Press the power button on the HMC to turn it on.
   b. If English is your language preference, continue with step 2e on page 57.
   c. If your language preference is something other than English, type the number 2 when you are prompted to change the locale.
Notes:
1) This prompt times out in 30 seconds if you do not act.
2) If your numerical keypad does not work, use the normal numerical keys instead.
d) Select the locale you want to display from the list in the Locale Selection window, and click OK. The locale identifies the language that the HMC interface displays.
e) Log in to the HMC using the following default user ID and password:
   ID: hsroot
   Password: abc123
   You will be prompted later to provide a new 7-character password for this ID.
f) To continue, accept the Hardware Management Console license agreements. If you decline the license agreement, you cannot complete the HMC configuration.
g) When the Guided Setup wizard is displayed, complete the wizard to configure the HMC. If the Guided Setup wizard is not displayed, you can access it manually from the HMC interface. See “Accessing the Guided Setup wizard using the HMC interface” on page 58.

After you have completed the Guided Setup wizard
1. After you have completed the Guided Setup wizard, complete the following tasks:
   a) Connect the managed system to a power source. The managed system will then power on its service processor. Once the service processor is powered on, proceed to the next step. This process will take 3 to 5 minutes. The following sequence of events signals that power has been applied to the service processor (with the exception of the model 9118-575 server and the 590 and 595 servers):
      1) Progress indicators, also referred to as checkpoints, appear on the control panel display while the system is being started. The display might appear blank for a few moments during this sequence.
      2) When the service processor has completed its power on sequence, the green power-on light blinks slowly and the output on the control panel display is similar to the following:
         01     N      V=F
         T
   b) Click Server and Partitions > Server management to view the status of your managed system. (For model 9118-575 server and the 590 and 595 servers, also click Server and Partitions > Frame management to view the status of the frame.) It may take a few minutes for the status to display.
c) If the status shows Pending Authentication, then go to step 14. If you receive the message Authentication Failed, or if you do not receive a message, see Chapter 7, “Troubleshooting HMC setup,” on page 87.

Note: If you did not configure your HMC as a Dynamic Host Configuration Protocol (DHCP) server, the HMC will not automatically detect the managed system. To detect the managed system, see Add another managed system and enter the IP address that you assigned to the managed server when it is requested.
d) Set passwords for the managed system. (For model 9118-575 server and the 590 and 595 servers, set passwords for the managed system and the frame.) Did you receive the messagePending Authentication?

   Yes: The HMC will prompt you to set the passwords for the managed system. If you are not prompted by the HMC to set these passwords after several minutes, right-click the server entry on the console. The window for setting passwords opens. Set the password for each as directed.

   No: Set the managed system passwords using the HMC interface:
   1) Set the managed system password. For instructions, see Update your platform password in the HMC online help. You can find this topic in the online help index under Update and Platform password.
2. Set the password for the Advanced System Management general user ID. For instructions, see Update your Advanced System Management (ASM) general password in the HMC online help.

3. Set the password for the Advanced System Management administration user ID. For instructions, see Update your Advanced System Management (ASM) administrator password in the HMC online help.

e. Access the ASMI to set the time of day on the system:
   1) **Access the ASMI using the HMC.**
   2) **Set the time of day on the system.**

f. **Start the managed system**

g. **Ensure that you have one logical partition on the managed system.** For instructions, see Creating logical partitions from the manufacturing default configuration.

h. **Optional:** Add another managed system

2. When you are finished configuring the HMC, complete the setup steps that apply to your situation:
   a. If you are installing a new server with your HMC, return to your initial server setup checklist and configure logical partitions or install one or more operating systems.
   b. **If you are not installing a new server at this time,** complete the optional tasks described in “Postconfiguration steps for the HMC” on page 64 to further customize your configuration.

**Accessing the Guided Setup wizard using the HMC interface**

If the Guided Setup wizard did not display when you started the HMC for the first time, complete the following steps to access the Guided Setup wizard using the HMC interface:

1. In the navigation area, expand the HMC you want to work with. HMCs are listed by hostname or IP address.

2. Click **Information Center and Setup Wizard.**

3. In the contents pane, click **Launch the Guided Setup wizard.**

**Configuring the HMC using the HMC configuration checklist**

Complete the following checklist to successfully set up your HMC. You will have to restart your HMC for the configuration settings to take effect, so you might want to print this checklist and keep it with you as you configure your HMC. The first section of the checklist, called HMC configuration checklist, contains all the tasks necessary to set up your HMC. The last step directs you to a topic that contains optional setup tasks to further configure your system.

This information contains references to tasks that are not included in this PDF. You can access the IBM eServer Hardware Information Center on the HMC or on the Web. On the HMC, the information center is in the **Information Center and Setup Wizard** folder. On the Web, the information center is at http://www.ibm.com/server/library/infocenter. Select a continent, your language preference, and eServer hardware.

**Prerequisites**

Before you begin this checklist, be sure to complete the configuration preparation activity described in “Gathering required configuration settings” on page 48.

**HMC configuration checklist**

- **Start the HMC**
- **If you have not yet done so** get HMC fixes to ensure that your HMC has the latest updates. Return to this checklist when you have completed this step.
- **Set the date and time**
- **Change predefined passwords**
- **Optional:** Create additional users and return to this checklist when you have completed this step.
HMC configuration checklist

Configure network connections:

- To configure LAN adapters, follow these steps (perform each task for each LAN adapter).
  
  **Note:** If you are connecting the HMC to the model 9118-575 server or the 590 or 595 managed servers, you must configure the HMC in a private DHCP network using the eth0 Ethernet connection.
  
  - Set the media speed
  - Select the network type
  - Unless the HMC you are setting up is an additional local HMC in your private service network or a remote HMC in your private or open network, configure the HMC as a Dynamic Host Configuration Protocol (DHCP) server.
  - If the HMC you are setting up is an additional local HMC in your private service network or a remote HMC in your private or open network, set the IP address.
  - If you selected the open network, change HMC firewall settings.
  - If you are using an open network and a fixed IP address, set identification information.
  - If you are using an open network and a fixed IP address, configure a routing entry as the default gateway.
  - If you are using an open network and a fixed IP address, configure domain name services.
  - If you are using a fixed IP address and have DNS enabled, configure domain suffixes.
  - Test the connection from the HMC to the managed system.
  - Set up your HMC to connect to IBM and return to this checklist when you have completed this step.
  - Connect the managed system to a power source. If you receive the message Authentication Pending, continue with the next step in this checklist.

If you receive the message Authentication Failed, or you do not receive a message, see Chapter 7, “Troubleshooting HMC setup,” on page 87.

Set passwords for the managed system:

- If you received the message Authentication Pending, the HMC will prompt you to set the passwords for the managed system.
  
  - If you did not receive the message Authentication Pending, complete the following steps to set the passwords for the managed system. (For model 9118-575 server and the 590 and 595 servers, set passwords for the managed system and the frame.)
    - Set the managed system password. For instructions, see Update your platform password in the HMC online help.
    - Set the password for the Advanced System Management general user ID. For instructions, see Update your Advanced System Management (ASM) general password in the HMC online help.
    - Set the password for the Advanced System Management administration user ID. For instructions, see Update your Advanced System Management (ASM) administrator password in the HMC online help.

Access the ASMI to set the time of day on the system:

- Access the ASMI using the HMC.
  
  - Start the managed system and return to this checklist when you have completed this step.
  - Ensure that you have one logical partition on the managed system. For instructions, see Creating logical partitions from the manufacturing default configuration.
  
  Optional: Add another managed system and return to this checklist when you have completed this step.

If you are installing a new server with your HMC, return to your initial server setup checklist and configure logical partitions or install one or more operating systems.

If you are not installing a new server at this time, complete the optional tasks described in “Postconfiguration steps for the HMC” on page 64 to further customize your configuration.

Changing the predefined passwords for hscroot and root user IDs
It is essential to your system’s security that you change all predefined passwords immediately.

1. In the navigation area, expand the HMC that you want to work with. HMCs are listed by hostname or IP address.
2. Expand HMC Management.
3. Click HMC Users.
4. In the contents pane, click Manage HMC users, roles, and access.
5. Click the User icon.
6. Right-click the hscroot icon to change the hscroot password or the root icon to change the root password.
7. Select Change Password.
8. Type the new password in the first field. The password must be a minimum of 7 characters in length.
9. Confirm the new password by typing it again in the Retype new password field.

Configuring network connections
Configure network connections to allow the HMC to talk to managed systems or logical partitions. Set the identification information, configure domain name services, and configure the LAN adapters.

Configuring LAN adapters: To configure LAN adapters, complete the following tasks in the order shown for each LAN adapter:
1. “Setting the media speed.”
2. “Selecting the network type.”
3. Unless the HMC you are setting up is an additional local HMC in your private service network or a remote HMC in your private or open network, see “Configuring the HMC as a DHCP server” on page 61.
4. If the HMC you are setting up is an additional local HMC in your private service network or a remote HMC in your private or open network, see “Setting the IP address” on page 61.
5. If you selected the open network, see “Configuring a routing entry as the default gateway” on page 62.
6. If you selected the open network, see “Changing HMC firewall settings” on page 62.

Setting the media speed: Specify the media speed and duplex mode of the Ethernet adapter:
1. In the navigation area, expand the HMC that you want to work with. HMCs are listed by hostname or IP address.
2. Expand HMC Management.
3. Click HMC Configuration.
4. In the contents pane, click Customize network settings.
5. Click the LAN Adapters tab.
6. Select the LAN adapter you want to work with and click Details.
7. Click the Lan Adapter tab.
8. In the Local area network information section, select the media speed.
9. Click OK.

Selecting the network type: You can connect your HMC to a private or open network. A private service network consists of the HMC and the managed systems. A private service network is restricted to consoles and the systems they manage, and is separate from your company network. An open network consists of your private service network and your company network. An open network might contain network endpoints in addition to consoles and managed systems, and might span across multiple subnets and network devices.

To select the network type, complete the following steps:
1. In the navigation area, expand the HMC that you want to work with. HMCs are listed by hostname or IP address.
2. Expand HMC Management.
3. Click HMC Configuration.
4. In the contents pane, click Customize network settings.
5. Click the LAN Adapters tab.
6. Select the LAN adapter that you want to work with and click **Details**.
7. Click the **Lan Adapter** tab.
8. In the Local area network information page, select **Private** or **Open**.
9. Click **OK**.

**Related concepts**

- [Private and open networks in the HMC environment” on page 15](#)

**Configuring the HMC as a DHCP server:** Dynamic Host Configuration Protocol (DHCP) provides an automated method for dynamic client configuration. Clients that are DHCP enabled automatically obtain their own IP address and configuration parameters from the server. In a private service network, configure your first or only HMC as a DHCP server. The HMC then provides nonroutable IP addresses to its managed systems. This allows the HMC to co-exist with other DHCP servers in your company network when you connect your private service network to an open network. For more information, see [“The HMC as a DHCP server” on page 19](#).

**Note:** If you are connecting the HMC to the model 9118-575 server or the 590 or 595 managed servers, you must configure the HMC in a private DHCP network using the eth0 Ethernet connection.

To configure the HMC as a DHCP server, complete the following steps:

1. In the navigation area, expand the HMC that you want to work with. HMCs are listed by hostname or IP address.
2. Expand **HMC Management**.
3. Click **HMC Configuration**.
4. In the contents pane, click **Customize network settings**.
5. Click the **LAN Adapters** tab.
6. Select the LAN adapter that you want to work with and click **Details**.
7. Click the **Lan Adapter** tab.
8. In the DHCP Server section, check **Enable DHCP Server** to enable the HMC as a DHCP server.
9. Enter the address range of the DHCP server.
10. Click **OK**.

**Setting the IP address:** Use the following steps to set your IP address:

1. In the navigation area, expand the HMC that you want to work with. HMCs are listed by hostname or IP address.
2. Expand **HMC Management**.
3. Click **HMC Configuration**.
4. In the contents pane, click **Customize network settings**.
5. Click the **LAN Adapters** tab.
6. Select the LAN adapter that you want to work with and click **Details**.
7. Click the **Lan Adapter** tab.
8. Select **Obtain an IP address automatically** or **Specify an IP address**.
9. If you selected to specify an IP address, enter the TCP/IP interface address and the TCP/IP interface network mask.
10. Click **OK**.
Changing HMC firewall settings: In an open network, a firewall usually controls outside access to your company network. The HMC also has a firewall on each of its Ethernet adapters. If you want to control the HMC remotely or give remote access to others, modify the firewall settings of the Ethernet adapter on the HMC that is connected to your open network.

To configure a firewall, use the following steps:
1. In the navigation area, expand the HMC that you want to work with. HMCs are listed by hostname or IP address.
2. Expand HMC Management.
3. Click HMC Configuration.
4. In the contents pane, click Customize network settings.
5. Click the LAN Adapters tab.
6. Select the LAN adapter that you want to work with and click Details.
7. Click the Firewall tab.
8. Using one of the following methods, you can allow any IP address using a particular applications through the firewall, or you can specify one or more IP addresses:
   • Allow any IP address using a particular application through the firewall:
     a. From the top box, highlight the application.
     b. Click Allow Incoming. The application displays in the bottom box to signify that it has been selected.
   • Specify which IP addresses to allow through the firewall:
     a. From the top box, highlight an application.
     b. Click Allow Incoming by IP Address.
     c. On the Hosts Allowed window, enter the IP address and the network mask.
     d. Click Add and click OK.
9. Click OK.

Setting identification information
Identification information includes the HMC’s hostname, the domain name, and the HMC’s description.

To identify your system to the network, complete the following steps:
1. In the navigation area, expand the HMC you want to work with. HMCs are listed by hostname or IP address.
2. Expand HMC Management.
3. Click HMC Configuration.
4. In the contents pane, click Customize network settings.
5. Click the Identification tab.
6. In the Console name field, enter the HMC’s hostname.
7. Enter the domain name.
8. In the Computer description field, enter the HMC’s description.
9. Click OK.

Configuring a routing entry as the default gateway
To configure a routing entry as the default gateway, use the following steps:
1. In the navigation area, expand the HMC you want to work with. HMCs are listed by hostname or IP address.
2. Expand HMC Management.
3. Click HMC Configuration.
4. In the contents pane, click Customize network settings.
5. Click the Routing tab.
6. In the Default gateway information section:
   a. Enter the gateway address of the routing entry you want to set as the default gateway.
   b. Enter the gateway device of the routing entry you want to set as the default gateway.
7. Click OK.

**Configuring domain name services**
Configure domain name services if you plan to set up an open network. Domain Name System (DNS) is a distributed database system for managing host names and their associated Internet Protocol (IP) addresses. Configuring domain name services includes enabling DNS and specifying the domain suffix search order.

1. In the navigation area, expand the HMC that you want to work with. HMCs are listed by hostname or IP address.
2. Expand HMC Management.
3. Click HMC Configuration.
4. In the contents pane, click Customize network settings.
5. Click the Name Services tab.
6. Check DNS enabled to enable DNS.
7. If you enabled DNS, specify the DNS server search order and the domain suffix search order.
8. Click OK.

**Configuring domain suffixes**
The list of domain suffixes is used to resolve an IP address starting with the first entry in the list.

The domain suffix is a string appended to a hostname that is used to help resolve its IP address. For example, a hostname of myname might not be resolved. However, if the string myloc.mycompany.com is an element in the domain suffix table, then there will be an attempt to also resolve myname.mloc.mycompany.com.

To configure a domain suffix entry, use these steps:
1. Enter a string to be used as a domain suffix entry.
2. Click Add to add it to the list.

**Testing the connection between the HMC and the managed system**
This option enables you to verify that you are properly connected to the network.

To test network connectivity, you must be a member of one of the following roles:
• super administrator
• service representative

To test network connectivity, do the following:
1. In the Navigation area, click the HMC Management icon.
2. In the Contents area, click the HMC Configuration icon.
3. In the Contents area, click Test Network Connectivity.
4. Type the host name or IP address of any system to which you want to connect.
5. Click OK.

To understand how the HMC can be used in a network, see “HMC network connections” on page 14.

For more information about configuring the HMC to connect to a network, see “Configuring the HMC using the HMC configuration checklist” on page 58.
Postconfiguration steps for the HMC

After you have installed and successfully configured the HMC, you can perform these optional tasks as necessary.

Optional: Postconfiguration tasks

- Back up the HMC
- Configure logical partitions
- Install the operating systems
- Access the operating systems using the HMC.
- Configure Capacity on Demand
Chapter 5. Installing and securing the remote client

You can access your Hardware Management Console (HMC) remotely by installing the remote client on your PC. The remote client provides flexibility by allowing you to manage your system from virtually anywhere you have a PC. Up to five remote clients can be logged in simultaneously. There are some tasks you cannot perform using the remote client. These tasks include determining the level of HMC code, restarting the HMC interface, and configuring System Manager Security for certificate authority or viewing overview and status information. System Manager Security ensures that the HMC can operate securely in client/server mode. Servers and clients communicate over the Secure Sockets Layer (SSL) protocol, which provides server authentication, data encryption, and data integrity.

To set up the remote client and secure the HMCs in your network, perform the following procedures for Web-based System Manager Remote Client for Java Web Start or the Web-based System Manager.

Web-based System Manager Remote Client for Java Web Start
1. “Configuring one HMC as a certificate authority” on page 66
2. “Generating private key ring files for the servers” on page 66
3. “Installing private key ring files on the servers” on page 66
4. “Distributing the certificate authority’s public key with Web-based System Manager Remote Client for Java Web Start” on page 67
5. “Viewing configuration properties” on page 69
6. “Configuring HMC object manager security” on page 69
7. “Installing the Web-based System Manager Remote Client for Java Web Start” on page 71
8. “Uninstalling the Web-based System Manager Remote Client for Java Web Start” on page 72

Web-based System Manager Remote Client
1. “Configuring one HMC as a certificate authority” on page 66
2. “Generating private key ring files for the servers” on page 66
3. “Installing private key ring files on the servers” on page 66
4. “Installing the Web-based System Manager Remote Client” on page 69
5. “Distributing the certificate authority’s public key with Web-based System Manager Remote Client” on page 68
6. “Viewing configuration properties” on page 69
7. “Configuring HMC object manager security” on page 69
8. “Uninstalling the Web-based System Manager Remote Client” on page 70

To install Web-based System Manager on AIX®, see the Web-based System Manager Administration Guide.

Related topics
System Manager Security
“Remote client comparison” on page 20
Configuring one HMC as a certificate authority

This procedure defines a system as an internal certificate authority (CA) for HMC security and creates a public key ring file for the CA that you can distribute to all of the clients that access the servers.

1. Verify that you are using a local HMC and not the Web-based System Manager Remote Client.
2. Ensure that you are logged in as the hscroot user at the HMC being configured as the internal CA.
3. In the navigation area, expand the local HMC. It is the first HMC in the list.
5. Click Certificate Authority.
6. In the System Manager Certificate Authority window, click Configure this system as a System Manager Certificate Authority. You can also select Configure from the Certificate Authority menu.
7. Use the help to guide you through completing the task.

Note: Remember the password you set for the CA private key file. You will need to use it when you generate private key ring files for the servers.

Generating private key ring files for the servers

Use the certificate authority (CA) to generate private key ring files for the servers. The private key ring file consists of the private key and the server certificate.

Note: If the system defined as a CA will also be used in server mode, you must complete the steps for generating and installing private key ring files on that system.

1. In the navigation area, expand the local HMC. It is the first HMC in the list.
2. Expand System Manager Security.
3. Click Certificate Authority.
4. In the System Manager Certificate Authority window, click Generate Servers’ Private Key Ring Files. You can also select Generate Keys from the Certificate Authority menu.
5. In the Password window, type the CA private key file password. This password was created when the HMC was configured as the CA.
6. Click OK.
7. In the Generate Server’s Private Key Ring Files window, use the help information to guide you through completing the task.
8. Click OK when you are finished.

Installing private key ring files on the servers

1. Copy the server private key ring files to diskette:
   a. In the navigation area, expand the local HMC. It is the first HMC in the list.
   b. Expand System Manager Security.
   c. Click Certificate Authority.
   d. In the System Manager Certificate Authority window, click Copy Servers’ Private Key Ring Files to diskette. You can also select Copy Servers’ Keys from the Certificate Authority menu.
   e. When the Copy Server’s Private Key to diskette dialog displays, insert a diskette.
   f. Click OK to copy the servers’ private key ring files to diskette.
2. Install the private key ring file on each server. Repeat the following steps for each server for which you generated a private key ring file:
   a. In the navigation area, expand the local HMC. It is the first HMC in the list.
   b. Expand System Manager Security.
   c. Click Server Security.
d. In the System Manager Server Security window, click **Install the private key ring file for this server.** You can also select **Install Key** from the Server menu.

e. In the Install Private Key Ring File window, select **diskette** as the source for the server private key ring file. Insert the diskette containing the server’s key into the diskette drive.

f. Click **OK**.

3. Configure the server as a secure System Manager server. Repeat the following steps for each server on which you installed a private key ring file:

   a. In the navigation area, expand the local HMC. It is the first HMC in the list. HMCs are listed by hostname or IP address.

   b. Expand **System Manager Security**.

   c. Click **Server Security**.

   d. In the System Manager Server Security window, click **Configure this system as a Secure System Manager server.** You can also select **Configure** from the Server menu.

   e. Use the help to guide you through completing the task.

**Distributing the certificate authority’s public key with Web-based System Manager Remote Client for Java Web Start**

If you are using the Web-based System Manager Remote Client for Java Web Start, use the following instructions to copy the certificate authority (CA) public key ring file (SMpubkr.zip) to each server that you will use to download the remote client.

**Note:** If the system defined as a CA will also be used in server mode, you must complete the steps for distributing the CA’s public key for that system. Although the CA public key was created on this system, it is not in the correct location for the system to be used as a server.

1. On the CA system, perform the following steps to copy the CA’s public key to diskette:

   a. In the navigation area, expand the local HMC. It is the first HMC in the list.

   b. Expand **System Manager Security**.

   c. Click **Certificate Authority**.

   d. In the System Manager Certificate Authority window, click **Copy this Certificate Authority’s Public Key Ring File to diskette.** You can also select **Copy out CA Public Key** from the Certificate Authority menu.

   e. When the Copy CA Public Key to Diskette window opens, insert a diskette.

   f. Select **HMC or AIX client** to write the file to a tar diskette.

   g. Click **OK** to copy the public key ring file.

2. Copy a CA’s public key from diskette to each server. Repeat the following steps for each client or server:

   a. In the navigation area, expand the local HMC. It is the first HMC in the list.

   b. Expand **System Manager Security**.

   c. Click **Certificate Authority**.

   d. In the System Manager Certificate Authority window, click **Copy another Certificate Authority’s Public Key Ring File from diskette.** You can also select **Copy in CA Public Key** from the Certificate Authority menu.

   e. When the Copy CA Public Key from Diskette window opens, insert the diskette that contains the copied CA’s public key ring file.

   f. Click **OK** to copy the public key ring file.
Distributing the certificate authority’s public key with Web-based System Manager Remote Client

If you are using the Web-based System Manager Remote Client, follow these instructions to copy the CA’s public key ring file (SM.pubkr) to the Web-based System Manager directory of each client:

1. The Web-based System Manager Remote Client must be installed on the client before proceeding. If you have not yet installed the Web-based System Manager Remote Client, perform the steps in “Installing the Web-based System Manager Remote Client” on page 69, and then return to these instructions.

2. On the CA system, perform the following steps to copy the CA’s public key to diskette:
   
a. If you plan to distribute the CA’s public key to an HMC or AIX client, ensure that the disk is a tar diskette.
      If you plan to distribute the CA’s public key to a PC client, ensure that the disk is formatted for DOS.
   
b. In the navigation area, expand the local HMC. It is the first HMC in the list.
   
c. Expand System Manager Security.
   
d. Click Certificate Authority.
   
e. In the System Manager Certificate Authority window, click Copy this Certificate Authority’s Public Key Ring File to diskette.
   
f. When the Copy CA Public Key to Diskette window opens, insert a diskette.
   
g. Select the type of client or server to which you want the public key ring file to be copied:
      • Select HMC or AIX client to write the file to a tar diskette.
      • Select PC client to write the file to a diskette in DOS file format.

   **Note:** Selecting PC Client writes the file to diskette in DOS file format.
   
h. Click OK to copy the public key ring file.

3. To copy a CA’s public key from diskette to each HMC client:
   Repeat the following steps for each client or server:
   
a. In the navigation area, expand the local HMC. It is the first HMC in the list.
   
b. Expand System Manager Security.
   
c. Click Certificate Authority.
   
d. In the System Manager Certificate Authority window, click Copy another Certificate Authority’s Public Key Ring File from diskette.
   
e. When the Copy CA Public Key from Diskette window opens, insert the diskette that contains the copied CA’s public key ring file.
   
f. Click OK to copy the public key ring file.

4. Distribute the CA’s public key to your Windows, Linux, or AIX remote clients using the following steps:
   Use command line or stand-alone tools to copy the CA’s public key from diskette to the codebase directory of the remote client. The CA’s public key file must be copied in binary format. The codebase directory locations are:
   
   • On a Windows client: Program files\websm\codebase
   • On an AIX client: /usr/websm/codebase
   • On a Linux™ client: /opt/websm/codebase
Viewing configuration properties

You can view the properties of the certificate authority (CA) and of any server. The property windows provide read-only information for the CA and the servers.

View CA properties
1. In the navigation area, expand the local HMC. It is the first HMC in the list.
2. Expand System Manager Security.
3. Click Certificate Authority.
4. Select Properties.
5. Type the password.

View server properties
1. In the navigation area, expand the local HMC. It is the first HMC in the list.
2. Expand System Manager Security.
3. Click Server Security.
4. Select View properties for this server from the task list.

Configuring HMC object manager security
1. In the navigation area, expand the local HMC. It is the first HMC in the list.
2. Expand System Manager Security.
3. Click Object Manager Security.
5. Select a socket mode.
6. Click OK.

If you are using the Web-based System Manager Remote Client for Java Web Start, install this product now. See “Installing the Web-based System Manager Remote Client for Java Web Start” on page 71.

Installing the Web-based System Manager Remote Client

1. [Uninstall] the previous version of the Web-based System Manager Remote Client.
2. Type the following address in your machine’s Web browser:
   
   http://<system name>/remote_client.html

   where system name is the name of the HMC you plan to access remotely.
3. Enter your HMC user ID and password.
4. Click InstallShield.
5. Click Windows to download the setup.exe file or click Linux to download the wsmlinuxclient.exe file.
6. If you are using a Linux system, run the following command to make the wsmlinuxclient.exe file executable:
   
   chmod 755 wsmlinuxclient.exe

   Run the wsmlinuxclient.exe file or the setup.exe file to begin the installation process. If you encounter problems with this step, see Troubleshooting for help.
7. When the Remote Client Installer window displays, click Next to continue.
8. To install using the default location, click Next. Otherwise, browse or type the desired location and click Next.
10. A confirmation window displays, showing you the installation location, the package being installed, and the approximate size of the installation package. If any of the information shown is incorrect, click Back to make corrections. Click Next to start the installation. A status window displays a message indicating the installation completed successfully or error messages if errors occurred during the installation. Click Finish to close the window.

11. Type the following address in your machine’s Web browser:
http://<system name>/remote_client_security.html

where system name is the name of the HMC you plan to access remotely.

12. Click Windows to download the setupsec.exe file or click Linux to download the setupsec1.exe file.

13. Run the setupsec.exe file or the setupsec1.exe file to begin the installation process. If you encounter problems with this step, see Troubleshooting for help.

14. When the Remote Client Security Installer window displays, click Next to continue.

15. To install using the default location, click Next. Otherwise, browse or type the desired location and click Next.

   Note: Be sure the location you select in this step is the same location that you selected when installing the remote client.

16. A confirmation window displays, showing you the installation location, the package being installed, and the approximate size of the installation package. If any of the information shown is incorrect, click Back to make corrections. Click Next to start the installation.

17. A status window displays a message indicating the installation completed successfully, or error messages if an error occurred during the installation. Click Finish to close the window.

   Note: To make a secure connection from the Remote Client, you must configure security on the HMC and copy the CA’s public key to the client. See Web-based System Manager Remote Client tasks

---

### Uninstalling the Web-based System Manager Remote Client

To install the latest version of the Web-based System Manager Remote Client, you must uninstall any previous versions from your Linux or Windows PC.

**Linux**

1. Run the following command:

   ```bash
   installdir/uninst/uninstall
   ```

   where installdir is the name of the directory where the remote client is located.

2. Run the following command:

   ```bash
   installdir/uninstssl/uninstallssl
   ```

   where installdir is the name of the directory in which your remote client resides.

**Windows**

Complete the following steps once to uninstall the Web-based System Manager Remote Client and again to uninstall remote client security:

1. From the task bar, select Start > Settings > Control panel.

2. In the Control window, double-click the Add/Remove Programs icon.

3. From the list of programs on the Install/Uninstall tab, select Web-Based System Manager Remote Client to uninstall the remote client and Remote Client Security to uninstall remote HMC client security.
Note: Earlier versions of the remote client might display as Web-based System Manager PC Client and the remote client security as Web-based System Manager PC Client Security.

4. Click Change/Remove to start the Uninstall wizard.
5. Click Next in the initial window.
6. Click Next in the Confirmation window.
7. A status window displays a message indicating that the uninstallation completed successfully or error messages if errors occurred during the uninstallation.
8. Click Finish to close the window.
9. Repeat steps 1 on page 70 through 8 to uninstall remote client security.

Installing the Web-based System Manager Remote Client for Java Web Start

Complete the following steps to install the Web-based System Manager Remote Client for Java Web Start:

1. Type the following address in your PC’s Web browser:
   
   http://<system name>/remote_client.html

   where system name is the name of the HMC you plan to access remotely.

2. Enter your HMC user ID and password.

3. From the Web-based System Manager Remote Client Selection page, click Java Web Start.

4. If you do not have Java Web Start currently installed on your client, click Java Web Start for Windows for a Windows client or Java Web Start for Linux for a Linux client on the Web-based System Manager Remote Client for Java Web Start Installation page to download the installation image. Download the most recent compatible version. Click on each version to see system requirements.
   - To install on a Windows client, double-click the downloaded image to launch the installation wizard.
   - To install on a Linux client, use the following command:
     
     ```
     rpm -i ibm-linux-jre.i386.rpm
     export PATH=$PATH:/opt/IBMJava2-142/jre/bin
     cd /opt/IBMJava2-142/jre/javaws/updateSettings.sh
     ```

   Note: The last line (/opt/IBMJava2-142/jre/javaws/updateSettings.sh) must be run from the root directory.

5. Go back to the Web-based System Manager Remote Client for Java Web Start Installation page and click Remote Client to download the remote client to your PC.


Note: If you installed the Web-based System Manager Remote Client for Java Web Start on a Linux system, launch Web-based System Manager one of the following ways:
   - Use a virtual terminal session to launch the Web-based System Manager Remote Client for Java Web Start:
     - a. Open a virtual terminal session and navigate to the directory in which you installed Java Web Start. This is usually the javaws directory.
     - b. Launch Java Web Start by executing the javaws command.
     - c. From the Java Web Start Application Manager, select View > Downloaded Applications.
     - d. Select Web-based System Manager Remote Client.
e. Select Application > Start Web-based System Manager to launch the remote client.

- Use the browser to launch the Web-based System Manager Remote Client for Java Web Start:
  a. Type the following address in your machine’s Web browser:
     \[
     \text{http://<system name>/remote_client.html}
     \]
     where \textit{system name} is the name of the HMC you plan to access remotely.
  b. Click Java Web Start.
  c. Click Remote Client.

\textbf{Note:} The installation of remote client security is included in the installation process for the Web-based System Manager Remote Client for Java Web Start.

---

**Uninstalling the Web-based System Manager Remote Client for Java Web Start**

Complete the following tasks to uninstall the Web-based System Manager Remote Client for Java Web Start from your PC:

1. From the View menu in the Java Web Start Application Manager, select \textbf{Downloaded Applications}.
2. Click the \textbf{Web-based System Manager Remote Client} icon.
3. Click \textbf{Application > Remove Application}.
Chapter 6. Working with the HMC

To learn more about the commands you can use to operate the HMC remotely, see Overview of HMC tasks.

These topics are intended for HMC users who want to perform actions on the HMC itself. For more information, click on the associated topic link:

“Basic operations”
Describes the basic operations that you can perform on your HMC, such as starting the HMC, changing the language HMC language, and logging off the HMC.

“Working with partition profile information” on page 76
Back up, restore, initialize, and remove profile information for the logical partitions.

“Back up and restoring the HMC” on page 78
Describes how to back up HMC data.

“Working with users, roles, and passwords” on page 81
This my description of this link.

“Using the HMC remote command line” on page 83
Provides information about using the command-line interface on the HMC.

Basic operations

This topic provides information on how to perform basic operations on your HMC:

“Starting the HMC”
Explains how to start the HMC interface

“Shutting down, rebooting, and logging off the HMC” on page 74
Explains how to shut down, reboot, and log off the HMC interface

“Setting the date and time” on page 74
Describes how to change the date and time for the HMC

“Changing the HMC interface language” on page 75
Describes how to change the interface language that you see on the HMC interface, as well as the locale

“Configuring the HMC keyboard layout” on page 75
Describes how to configure the keyboard layout

“Viewing recent HMC activity” on page 76
Explains how to view recent HMC activity

Starting the HMC

To start the HMC, do the following:
1. Press the power button on the HMC to turn it on.
2. If English is your language preference, continue with step 5 on page 74
3. If your language preference is something other than English, type the number 2 when you are prompted to change the locale.

   **Note:** This prompt times out in 30 seconds if you do not act.

4. Select the locale that you want to display from the list in the Locale Selection window, and click **OK**. The locale identifies the language that the HMC interface displays.

5. Log in to the HMC using the following default user ID and password:
   
   ID: hscroot
   
   Password: abc123

6. Press **Enter**.

**Shutting down, rebooting, and logging off the HMC**

This task allows you to shut down, reboot, and log off the HMC interface.

**Attention:** Only use the white button on the HMC to perform a manual shut down if the server does not respond to any tasks performed from the console, such as shutting down the HMC.

If an operating system is open and running on a partition, and you decide to shut down, reboot, or log off the HMC interface, the operating system continues to run without interruption.

To log off the HMC interface, do the following:

1. In the main menu, click **Console > Exit**. At this point, you can select to save the state of the console for the next session by selecting the check box next to the option.

   **Note:** When you exit from the HMC session locally, you can select to shut down, reboot, or log off your session. The following is a description of each option:

   **Shutdown Console**
   
   Powers off the HMC

   **Reboot Console**
   
   Shuts down the HMC and then reboots it to the login prompt

   **Logout**
   
   Returns the user to the login prompt without shutting down the HMC

2. Click **Exit Now**.

**Setting the date and time**

The battery-operated clock keeps the date and time for the HMC. You might need to reset the console date and time if the battery is replaced, or if you physically move your system to a different time zone. If you change the date and time information, the change does not affect the systems and logical partitions that the HMC manages.

To change the date and time for the HMC, do the following:

1. Ensure that you are a member of one of the following roles:
   
   - Super administrator
   - Service representative
   - Operator
   - Viewer

2. In the navigation area, expand the HMC you want to work with. HMCs are listed by hostname or IP address.

3. Expand **HMC Management**.

4. Click **HMC Configuration**.
5. In the contents pane, click **Customize Console Date and Time**.
6. Enter the date, time, and time zone, and click **OK**.

**Note:** The time setting will automatically be adjusted for daylight saving time in the time zone you select.

**Changing the HMC interface language**

When you power on the HMC, the HMC prompts you to change the interface language and locale. The `locale` is the language in which you want the HMC to display. Changes made using this procedure affect the language and locale for the HMC server. If you are using the remote client to connect to the HMC, the language and locale settings on your Windows operating system determine the settings that the remote client uses to display the HMC on your PC.

Any user role can change the HMC interface language.

To change the HMC interface language and locale when you power on the HMC, do the following:

1. Power on the HMC.
2. When you are prompted to change the language and locale, select the language and locale you want to display. If nothing is selected within 20 seconds, the dialog exits. By default, the **Exit now and prompt again for locale change** option is selected. The boot continues.
3. Click **OK**. When the HMC completes the power-on process, the language and locale that you selected are displayed.

To change the HMC interface language and locale using the HMC Configuration application, do the following:

1. In the Navigation area, click the **HMC Management** icon.
2. In the Contents area, double-click the **HMC Configuration** icon.
3. In the Contents area, click **Change Current Language and Locale**.
4. In the window, select the language and locale you want to display.
5. Click **OK**.
6. Log off the HMC interface and then log in.

**Configuring the HMC keyboard layout**

When you power on the HMC, the HMC prompts you to configure the keyboard layout. If you do not respond, the HMC continues to power on using previous keyboard configuration. English is the default setting.

Any user role can change the keyboard layout.

**Note:** If you previously selected the **Do not run this program to change keyboard layout on the next system boot** option and you want to change the keyboard layout again, open an rshterm and use the following `chhmc` command:

```
chhmc -c kbdcfg -s enable
```

To configure the keyboard layout when you power on the HMC, do the following:

1. Power on the HMC.
2. When the Keyboard Layout Configuration Screen displays, select the **Change to a new keyboard layout** option. If nothing is selected within 20 seconds, the dialog exits. By default, the **Do not change keyboard layout and run this program again on the next system boot** option is selected. The boot continues.
3. Select the desired keyboard layout from the list.
4. Select the appropriate option if you want to run this program on the next system boot and press Enter.

**Viewing recent HMC activity**

To see a log of recent HMC activity, you can view console events. Each event has an associated time stamp.

The following is a sample of the events recorded:

- When a logical partition was activated
- When a system was powered on
- When a logical partition was shut down
- Results of a scheduled operation

To view console events, you must be a member of one of the following roles:

- super administrator
- service representative
- operator
- product engineer

To view console events, do the following:

1. In the Navigation area, click the HMC Management icon.
2. In the Contents area, click the HMC Configuration icon.
3. In the Contents area, select View Console Events.

**Working with partition profile information**

You can back up, restore, initialize, and remove profiles that you have created. This topic describes each of these options.

For more information about creating profiles, see Creating new logical partitions and partition profiles

"Backing up partition profile data"
Describes how to back up profile data on the HMC

"Initializing profile data” on page 77
Explains how to initialize the profile data

"Restoring profile data” on page 77
Explains how to read the profile data from the previously backed-up file on the HMC and load this data to the managed system

"Removing profile data” on page 77
Explains how to remove the previously backed-up file on the HMC

**Backing up partition profile data**

This topic describes how to back up logical partition profile data.

To back up partition profile data, you must be a member of one of the following roles:

- super administrator
- service representative

To back up partition profile data, do the following:
1. In the Contents area, select the managed system.
2. From the menu, click Selected > Profile Data > Backup.
3. Type the name you want to use for this backup file.
4. Click OK.

**Initializing profile data**

When you initialize profile data, you return the managed system to a state that does not have any logical partitions or profiles. You can perform this task in order to stabilize your managed system if the profile data becomes corrupt.

**Attention:** After you perform this task, any profiles that you created prior to initialization are erased. Use this procedure only under the direction of your service provider.

To initialize profile data, your authority level must be a super administrator.

**Note:** You can initialize profile data only when the managed system is in the *Operating* or *Standby* state and all the partitions are in the *Not Activated* state.

To initialize profile data, do the following:
1. In the Contents area, select the managed system.
2. From the menu, select Selected > Profile Data > Initialize.
3. Click Yes.

**Restoring profile data**

Selecting this menu item restores profile data to the HMC from a backup file stored on the HMC hard drive.

**Note:** This is not a concurrent procedure. When the data is restored, the managed system powers on to Partition Standby. For more information about power-on modes, see [Managed system power-on modes](#).

To restore stored profile data on the HMC hard drive, you must be a member of one of the following roles:

- super administrator
- service representative

To restore profile data, do the following:
1. In the Contents area, select the managed system.
2. From the menu, select Selected > Profile Data > Restore.
3. Select the profile information that you want to restore from the list of backup files.
4. Select a restore option.
5. Click OK.

**Removing profile data**

To remove stored profile data from the HMC hard disk drive, you must be a member of one of the following roles:

- super administrator
- service representative

To remove stored profile data, do the following:
1. In the Contents area, select the managed system.
2. From the menu, select Selected > Profile Data > Remove.
3. Select the profile data that you want to remove.
4. Click OK.

**Backing up and restoring the HMC**

The HMC provides the tools you need to back up and restore important HMC data.

"Back up critical HMC data"  
Describes how to back up important console information to DVD, a remote system mounted to the HMC file system (such as NFS), or a remote site through FTP

"Restoring critical HMC data" on page 79  
Describes how to restore critical HMC data

"Scheduling and reviewing HMC backups" on page 80  
Explains how to schedule backups of important console information

"Saving HMC upgrade data" on page 80  
Explains how to save upgrade data so that you can reinstall it if the HMC must be recovered

"Reinstalling the HMC machine code" on page 80  
Explains how to reinstall the HMC machine code prior to restoring critical backup data and it describes how to reinstall the HMC interface onto the HMC PC and install backup information.

Backing up the HMC does not back up the data on the server. For more information about backing up data on a logical partition, select the topic that matches your logical partition’s configuration:

- **Back up and recovering i5/OS data**  
  These topics provide instructions for backing up and restoring i5/OS installations.

- **Back up and recovering AIX logical partitions**  
  These topics provide instructions for backing up and restoring AIX installations.

- **Back up and recovering Linux installations**  
  These topics provide instructions for backing up and restoring Linux installations.

**Back up critical HMC data**

Using the HMC, you can back up all important data, such as the following:

- User-preference files
- User information
- HMC platform-configuration files
- HMC log files

**Note:** The archived data should be used *only* in conjunction with a reinstalation of the HMC from the product CDs. For information about how to reinstall the HMC, see "Reinstalling the HMC machine code" on page 80.

The Backup function saves the HMC data stored on the HMC hard disk to DVD, a remote system mounted to the HMC file system (such as NFS), or a remote site through FTP. Back up the HMC after you have made changes to the HMC or to the information associated with logical partitions.

**Note:** The DVD must be formatted in the DVD-RAM format before data can be saved to the DVD.

To back up the HMC, you must be a member of one of the following roles:
To back up the HMC, do the following:

1. In the Navigation area, click the **Licensed Internal Code Maintenance** icon.
2. In the Contents area, click the **HMC Code Update** icon.
3. Select **Back up Critical Console Data**.
4. Select an archive option. You can back up to DVD on the HMC, back up to a remote system mounted to the HMC file system (such as NFS), or a remote site through FTP.
5. Follow the instructions on the panel to back up the data.

### Restoring critical HMC data

The HMC backup data should be restored *only* in conjunction with a reinstallation of the HMC. For information about how to reinstall the HMC, see “Reinstalling the HMC machine code” on page 80.

**Note:** For this operation, you must have the backup DVD-RAM media or access to the remote server where the archive was created by using the procedure in “Backing up critical HMC data” on page 78.

To restore the HMC data, you must be a member of one of the following roles:

- super administrator
- operator
- service representative

Select the data-restoration procedure based on the data archiving method used:

- **Restoring from DVD**
  - Restore data that was archived to DVD.
- **Restoring from a remote server**
  - Restore data that was archived to a remote FTP or NFS sever.

### Restoring from DVD

If the critical console data has been archived on a DVD-RAM, do the following:

1. Select **1 - Restore Critical Console Data** from the menu displayed. This menu is displayed at the end of the HMC reinstallation.
2. Insert the DVD-RAM containing the archived console data. On first boot of the newly installed HMC, the data automatically restores.

### Restoring from a remote server

If the critical console data has been archived remotely, do the following:

1. Manually reconfigure network settings to enable access to the remote server after the HMC is newly installed. For information about configuring network settings, see “Configuring the HMC” on page 53.
2. In the Navigation area, click the **Licensed Internal Code Maintenance** icon.
3. In the Contents area, click the **HMC Code Update** icon.
4. Select **Restore Remote Console Data**.
5. Select the type of remote restore.
6. Follow the directions on the panel to restore the critical console data. The data automatically restores from the remote server when the system is rebooted.
Scheduling and reviewing HMC backups

You can schedule a backup to DVD to occur once, or you can set up a repeating schedule. You must provide the time and date that you want the operation to occur. If the operation is scheduled to repeat, you must select how often you want this backup to run (hourly, daily, weekly, or monthly).

Note: Only the most-recent backup image is stored at any time on the DVD.

To schedule a backup operation, do the following:
1. In the Navigation area, expand the HMC Management folder.
2. In the Navigation area, click the HMC Configuration icon.
3. In the Contents area, click Schedule Operations.
4. From the list, select the HMC you want to back up and click OK.
5. Select Options > New.
6. In the Add a Scheduled Operation window, select Backup Critical Console Data and click OK.
7. In the appropriate fields, enter the time and date that you want this backup to occur.
8. If you want this scheduled operation to repeat, click the Repeat tab and select the intervals at which you want the backup to repeat and press Enter.
9. When you have set the backup time and date, click Save. When the Action Completed window opens, click OK. A description of the operation displays in the Scheduled Operations window.

Saving HMC upgrade data

You can save the current HMC configuration in a special disk partition on the HMC. You should only save upgrade data immediately prior to upgrading your HMC software to a new release. This allows you to restore HMC configuration settings after upgrading.

Note: The special disk partition can hold only one level of backup data. Every time you perform this task, previous backup data is overwritten by the latest backup. To proceed with the upgrade after saving upgrade data, you can must place the new HMC recovery CD in the DVD drive and immediately reboot the HMC. Any configuration changes on the HMC after you saved upgrade data will not be saved.

To save upgrade data, do the following:
1. Expand the Licensed Internal Code Maintenance folder, then select the HMC application in the Navigation area.
2. Select the Save Upgrade Data task in the content area. An information window opens that prompts you to select the media (hard drive or DVD).
3. Select the appropriate media.
4. Click Continue.
5. Click OK to confirm and close the information window.

Reinstalling the HMC machine code

If the HMC is not responding, you can use the recovery CD to reinstall the HMC interface onto the HMC PC. After you reinstall the HMC machine code, you can restore the backup data that you created to recover your critical console information. For information about how to restore the HMC backup data, see "Restoring critical HMC data" on page 79.

To reinstall the HMC machine code, you must be a member of one of the following roles:
• super administrator
• operator
• service representative
To reinstall the HMC machine code, do the following:

1. Shut down and power off the HMC. For more information, see “Shutting down, rebooting, and logging off the HMC” on page 74.

2. Power on the HMC console and insert the HMC recovery CD. The HMC powers on from the media and displays the recovery panel.

3. Press F8 to select the 1 - Install/Recover option.

4. When the following message is displayed, press F1:
   PRESS F1 TO CONTINUE WITH THE RESTORE /PRELOAD PROCESS. PRESS ESC TO EXIT THE PROCESS.

5. After the installation of the first CD completes, you are prompted to insert the second installation CD into the DVD drive. Press any key to continue. The HMC reboots.

6. After the installation of the second CD completes, select 1 - Install additional software from CD media from the menu displayed to install the information center from the third CD.

7. After the information center installation, select 1 - Restore Critical Console Data from the menu displayed to restore data from a DVD. To restore from a remote server, select 2 - Finish the Installation.

---

**Working with users, roles, and passwords**

The following topics provide essential supporting information regarding HMC user administration tasks:

- "Creating an HMC user"
  Describes how to create HMC users

- "Viewing an HMC user description” on page 82
  Describes how to view HMC user definitions

- "Copying HMC user information” on page 82
  Describes how to copy an existing user information

- "Deleting an HMC user” on page 82
  Describes how to delete an HMC user

- "Creating a customized HMC role” on page 82
  Describes how to create a customized HMC role

- "Editing HMC user information and roles” on page 82
  Describes how to change HMC user description

- "Changing HMC user passwords” on page 82
  Describes how to change an existing HMC user’s password

---

**Creating an HMC user**

You can create various users using the HMC. The hscroot, root, and hscpe user IDs are special, or reserved. The hscpe user should only be created for use by your service provider when performing problem determination.

To create a user, do the following:

1. In the Navigation area, expand the HMC Management folder.
2. Click the HMC users icon.
3. In the Contents area, click Manage HMC Users and Access. The User Profiles window opens.
4. Click User > Add. Fill in the appropriate fields and click OK.
Viewing an HMC user description
To view a user description, do the following:
1. In the Navigation area, expand the HMC Management folder.
2. Click the HMC users icon.
3. In the Contents area, click Manage HMC Users and Access. The User Profiles window opens.
4. Click User > Modify. The current user description is displayed.

To read about the tasks each HMC user role can perform and the commands associated with each task, see [Overview of HMC tasks](#).

Copying HMC user information
To copy HMC user information, do the following:
1. In the Navigation area, expand the HMC Management folder.
2. Click the HMC users icon.
3. In the Contents area, click Manage HMC Users and Access. The User Profiles window opens.
4. Click User > Copy. Fill in the appropriate fields and click OK.

Deleting an HMC user
To delete a user, do the following:
1. In the Navigation area, expand the HMC Management folder.
2. Click the HMC users icon.
3. In the Contents area, click Manage HMC Users and Access. The User Profiles window opens.
4. Select the user that you want to remove.
5. Click User > Remove. The Delete Item Verification window opens.
6. Click Yes.

Creating a customized HMC role
To create a customized HMC role, do the following:
1. In the Navigation area, expand the HMC Management folder.
2. Click the HMC users icon.
3. In the Contents area, click Manage Access Task Roles and Managed Resource Roles. The Customized User Controls window opens.
4. Click the Task Roles radio button.
5. Click File > Add. The Add Role window opens.
6. Fill in the appropriate fields and click OK.

Editing HMC user information and roles
To edit HMC user information and roles, do the following:
1. In the Navigation area, expand the HMC Management folder.
2. Click the HMC users icon.
3. In the Contents area, click Manage HMC Users and Access. The User Profiles window opens.
4. Click User > Modify. Fill in the appropriate fields and click OK.

Changing HMC user passwords
To change HMC user passwords, do the following:
1. In the Navigation area, expand the HMC Management folder.
2. Click the HMC users icon.
3. In the Contents area, click Manage HMC Users and Access. The User Profiles window opens.
4. Click User > Modify. Fill in the new password and click OK.

**Using the HMC remote command line**

The command-line interface is useful in the following situations:

- When consistent results are required. If you have to administer several managed systems, you can achieve consistent results by using the command-line interface. The command sequence can be stored in scripts and run remotely.
- When automated operations are required. After you have developed a consistent way to manage the managed systems, you can automate the operations by invoking the scripts from batch-processing applications, such as the cron daemon, from other systems.

This topic provides information about using the command line interface on the HMC.

"Viewing HMC remote command information"
Describes the remote command line

"Setting up secure script execution between SSH clients and the HMC"
Describes how to ensure that the script executions between SSH clients and the HMC are secure

"Enabling and disabling HMC remote commands" on page 84
Explains how to enable or disable the remote command-line interface access to the HMC using the SSH facility

**Viewing HMC remote command information**

To view command information, type man and then the command name. For example, to learn more about the "Create a user for the HMC" (mkhmcusr) command, type the following at the command-line:

```
man mkhmcusr
```

**Setting up secure script execution between SSH clients and the HMC**

**Note:** To enable unattended script execution between an SSH client and an HMC, the SSH protocol must already be installed on the client’s operating system.

HMCs typically are placed inside the machine room where managed systems are located, so you might not have physical access to the HMC. In this case, you can remotely access it using either the remote client or the remote command-line interface. This topic describes how to ensure that your script executions between SSH clients and the HMC are secure.

To enable unattended script execution between an SSH client and an HMC, do the following:
1. In the Navigation area, select HMC Management.
2. In the Navigation area, click HMC Configuration.
3. In the Contents area, click Enable/Disable Remote Command Execution.
4. When the window opens, select the box to enable SSH.
5. Create an HMC user with one of the following roles:
   - super administrator
   - service representative
6. On the client’s operating system, run the SSH protocol key generator. To run the SSH protocol key generator, do the following:
   a. To store the keys, create a directory named $HOME/.ssh (either RSA or DSA keys can be used).
b. To generate public and private keys, run the following command:

```
ssh-keygen -t rsa
```

The following files are created in the $HOME/.ssh directory:
```
private key: id_rsa
public key: id_rsa.pub
```

The write bits for both group and other are turned off. Ensure that the private key has a permission of 600.

7. On the client’s operating system, use ssh and run the `mkauthkeys` command to update the HMC user’s `authorized_keys2` file on the HMC by using the following command:

```
ssh userid@hostname "mkauthkeys --add '<the key string from $HOME/.ssh/id_dsa.pub>'"
```

**Deleting the key from the HMC**

To delete the key from the HMC, select one of the following procedures:

You can use this procedure to modify various files in order to delete the key from HMC:

1. On the logical partition, use the `scp` command to copy the `authorized_keys2` file from the HMC to the logical partition, as follows:

```
scp userid@hostname:/.ssh/authorized_keys2 /tmp/mykeyfile
```

2. In the `/tmp/mykeyfile` file, remove the line that contains the key and host name of the system that you want to be able to run HMC commands remotely. The `ssh` command can then be run without being prompted for a password.

3. On a logical partition, use the `scp` command to copy the new file to the HMC:

```
scp /tmp/mykeyfile userid@hostname:/.ssh/authorized_keys2
```

4. If you want to enable password prompting for all hosts that access the HMC through `ssh`, use the `ssh` command to remove the key file from the HMC:

```
scp userid@hostname:.ssh/authorized_keys2 authorized_keys2
```

5. Edit the `authorized_keys2` file and remove all lines in this file, then copy it back to the HMC. For example:

```
scp authorized_keys joe@somehost:.ssh/authorized_keys2
```

OR

To use the command line to delete the key from the HMC, use the `mkauthkeys` command. For example:

```
ssh userid@hostname "mkauthkeys --remove 'joe@somehost'
```

**Enabling and disabling HMC remote commands**

You can enable or disable the remote command-line interface access to the HMC using the SSH facility.

To enable or disable remote commands, you must be a member of one of the following roles:

- super administrator
- service representative

To enable or disable remote commands, do the following:

1. In the Navigation area, click the **HMC Management** icon.
2. In the Contents area, double-click the **HMC Configuration** icon.
3. In the Contents area, click **Enable/Disable Remote Command Execution**.
4. Select the appropriate check box.
5. Click **OK**.

To disable the firewall that is enabled by default, you must access the network settings on the HMC.

To disable the HMC firewall, see “Changing HMC firewall settings” on page 62.
Chapter 7. Troubleshooting HMC setup

The following topics contain information about common problems that occur during the setup of the Hardware Management Console (HMC). The topics also contain common resolutions to those problems. The first topic applies to the HMC in general. The second topic applies to the remote client.

Setting up the HMC

Problem: You configured the HMC as a DHCP server, but the HMC did not automatically discover the managed system.

Resolution: Usually this means that the managed system was connected to a power source before the HMC was configured as the DHCP server. This caused the managed system to initialize to its IP address to the default values (HMC1 as 192.168.2.147 and HMC2 as 192.168.3.147) instead of waiting for an address from the HMC.

To correct the configuration on model 9118-575 server or the 590 or 595 managed servers, contact your service provider.

To correct the configuration for the model 520, 550, and 570 managed servers, complete the following tasks:
1. Shut down the managed system by pressing and holding the power button.
2. Remove the connection between the managed system and its power source.
3. Reconnect the managed system to its power source. The HMC automatically discovers the managed system.

If you had changed the IP address of the service processor using the ASM interface, use one of the following procedures for your model:

Model 520
1. Shut down the managed system by pressing and holding the power button.
2. Remove the connection between the managed system and its power source.
3. Remove the connection between the HMC and its power source.
4. Remove the service processor assembly as instructed in the "Remove the model 520 service processor assembly" topic. Begin with the step following "Disconnect the power source...". When you have removed the service processor, proceed to the next step.
5. To reset the service processor assembly, move both service processor reset toggle switches from their current position to the opposite position. See Figure 14 on page 88.
6. Reinsert the service processor into the managed system. For instructions, see Replace the model 520 service processor assembly.

7. Reconnect the HMC to its power source and start the HMC.

8. Log on to the HMC.

9. Reconnect the managed system to its power source. The HMC automatically discovers the managed system.

Model 550:

1. Shut down the managed system by pressing and holding the power button.

2. Remove the connection between the managed system and its power source.

3. Remove the connection between the HMC and its power source.

4. The service processor switch is located beneath the second power supply. To access the service processor switch, you must remove the second power supply. For instructions, see Remove the model 550 power supply.

5. To reset the service processor, move the service processor reset toggle switch A from its current position to the opposite position. See Figure 15 on page 89.
6. Reinsert the power supply into the managed system. For instructions, see Replace the model 550 power supply.

7. Reconnect the HMC to its power source and start the HMC.

8. Log on to the HMC.

9. Reconnect the managed system to its power source. The HMC automatically discovers the managed system.

Model 570:

1. Shut down the managed system by pressing and holding the power button.
2. Remove the connection between the managed system and its power source.
3. Remove the connection between the HMC and its power source.
4. To remove the service processor assembly, follow the instructions in the Remove the model 570 service processor assembly topic. Begin with the step following "Disconnect the power source..." in the instructions. When you have removed the service processor, proceed to the next step.

5. Reset the service processor by moving both service processor reset jumpers A from their current position to the opposite position. See Figure 16.

Figure 16. Model 570 service processor switch

6. Reinsert the service processor into the managed system. See Replace the model 570 service processor assembly.

7. Reconnect the HMC to its power source and start the HMC.

8. Log on to the HMC.

9. Reconnect the managed system to its power source. The HMC automatically discovers the managed system.

Problem: After setting up the HMC, the managed system’s status is Authentication Failed.

Resolution: Usually this means that the managed system password was set prior to HMC configuration. In this situation, the HMC does not recognize the managed system password and cannot access the managed system. To correct this situation, update the password on the managed system.

Installing the remote client

Problem: The wsmlinuxclient.exe or the setupsec1.exe file does not run.

Resolution: Modify the permissions on the file so that you have execute permissions. To modify the permissions, type the following command at the command prompt:

    chmod 755 filename

Problem: Changes do not take effect immediately after installing the Web-based System Manager Remote Client or the remote client security on a Linux system

Resolution: Perform one of the following tasks:
• Log off your current session and log in again
• Source your \texttt{/etc/profile} file

\textbf{Problem: You receive an error message that you cannot complete a connection}

\textbf{Resolution: If you receive a message such as the following:}

\begin{itemize}
  \item Cannot complete connection to hostname myhmc.
  \item Host myhmc is not a valid hostname.
  \item Host myhmc is not currently operating or is not connected to the network.
  \item Host myhmc is not running an operating system with a version of Web-based System Manager that is compatible with your client version of Web-based System Manager.
  \item The time to connect could have exceeded the time limit set in the websm.cfg file (remote_timeout).
  \item The inetd subsystem on host myhmc may not have been initialized on the 9090 port to start the WServer.
\end{itemize}

Additional information might be in the file \texttt{/var/websm/data/wserver.log} on host myhmc.

Possible solutions include the following tasks:

1. Sign on to the HMC you are trying to access remotely and verify that myhmc is the hostname of that HMC.
2. Locate the HMC that you are trying to access remotely and verify that it is operating and connected to the network.
3. Ensure that the version of the Web-based System Manager of the HMC you are trying to access remotely is the same version as the Web-based System Manager Remote Client.
4. The time it takes for your remote client to connect to the HMC you want to manage remotely has exceeded the time limit. To solve this problem, improve your connection speed. To do this, you might have to change the way in which the remote client and the HMC you want to manage remotely are connected.
5. The following reasons are most common for this message:
   \begin{itemize}
     \item You might have exceeded the limit of remote connections allowed to the HMC you are trying to access remotely.
     \item By default, the HMC uses a connect port of 9090 to handle the initial login communication. If you cannot enter your user ID and password, it means that you cannot connect to the 9090 port. Often this is because too many sessions were cancelled improperly and the 9090 port is overloaded. Restart the HMC you are trying to access remotely to cancel remote sessions that were improperly disconnected.
   \end{itemize}
Chapter 8. Related information

Listed below are Web sites and information center topics that relate to the Managing the Hardware Management Console topic collection.

Web site

The Web-based System Manager Remote Client can be installed on AIX, Linux, or the HMC. For more information about installing and using Web-based System Manager on AIX, see the Web-based System Manager Administration Guide (www.boulder.ibm.com/pseries/en_US/infocenter/base/aix52.htm#sysmgmt).

Other information

• Managing your server using the HMC
• Initial server setup
• Adding another console:
  – Advanced System Management Interface
  – Operations Console
  – Twinaxial console
• Customer service and support
• Migrating or upgrading your server

Saving PDF files

To save a PDF on your workstation for viewing or printing:
1. Right-click the PDF in your browser (right-click the link above).
2. Click Save Target As... if you are using Internet Explorer. Click Save Link As... if you are using Netscape Communicator.
3. Navigate to the directory in which you would like to save the PDF.
4. Click Save.

Downloading Adobe Acrobat Reader

You need Adobe Acrobat Reader to view or print these PDFs. You can download a copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html).
Appendix. Notices

This information was developed for products and services offered in the U.S.A.

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

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: THIS INFORMATION IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. The manufacturer 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 Web sites not owned by the manufacturer are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this product and use of those Web sites is at your own risk.

The manufacturer may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning products not produced by this manufacturer was obtained from the suppliers of those products, their published announcements or other publicly available sources. This manufacturer has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to products not produced by this manufacturer. Questions on the capabilities of products not produced by this manufacturer should be addressed to the suppliers of those products.

All statements regarding the manufacturer’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.
The manufacturer’s prices shown are the manufacturer’s suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

The drawings and specifications contained herein shall not be reproduced in whole or in part without the written permission of the manufacturer.

The manufacturer has prepared this information for use with the specific machines indicated. The manufacturer makes no representations that it is suitable for any other purpose.

The manufacturer’s computer systems contain mechanisms designed to reduce the possibility of undetected data corruption or loss. This risk, however, cannot be eliminated. Users who experience unplanned outages, system failures, power fluctuations or outages, or component failures must verify the accuracy of operations performed and data saved or transmitted by the system at or near the time of the outage or failure. In addition, users must establish procedures to ensure that there is independent data verification before relying on such data in sensitive or critical operations. Users should periodically check the manufacturer’s support websites for updated information and fixes applicable to the system and related software.

---

**Trademarks**

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

AIX
Electronic Service Agent
eServer
IBM

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

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

Other company, product or service names may be trademarks or service marks of others.

---

**Communications statements**

The following Class A statements apply to the IBM eServer i5 and eServer p5 servers, and to the IBM eServer OpenPower servers, with the exception of those that are specifically identified as Class B.

The following Class B statements apply to model 9111-520 (stand-alone version).
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.

Responsible Party:

International Business Machines Corporation
New Orchard Road
Armonk, NY 10504

Telephone: 1-919-543-2193

Industry Canada Compliance Statement

This Class A digital apparatus meets the requirements of the Canadian Interference-Causing Equipment Regulations.

Avis de conformité à la réglementation d’Industrie Canada

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC 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.

Australia and New Zealand Class A statement

Attention: 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
The following is a summary of the VCCI Japanese statement in the box above.

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

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

Per GB 9254–1998, the user manual for a Class A product must carry the following warning message (English translation from the Chinese standard) about use in a residential environment in Chinese (Simplified Chinese):

<table>
<thead>
<tr>
<th>声明</th>
</tr>
</thead>
<tbody>
<tr>
<td>此为 A 级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。</td>
</tr>
</tbody>
</table>

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

The following is a summary of the EMI Taiwan 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.

Radio Protection for Germany


Der Aussteller der Konformitätserklärung ist die IBM Germany.

Dieses Gerät erfüllt die Bedingungen der EN 55022 Klasse A. Für diese von Geräten gilt folgende Bestimmung nach dem EMVG:
Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an IBM authorized dealer or service representative for help.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Proper cables and connectors are available from IBM authorized dealers. IBM is not responsible for any radio or television interference caused by using other than recommended cables or 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 interferences, and (2) this device must accept any interferences received, including interference that may cause undesired operation.

Responsible Party:

International Business Machines Corporation
New Orchard Road
Armonk, NY 10504

Telephone: 1-919-543-2193

Industry Canada Compliance Statement

This Class B digital apparatus meets the requirements of the Canadian Interference-Causing Equipment Regulations.

Avis de conformité à la réglementation d’Industrie Canada
Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

**European Community Compliance Statement**

This product is in conformity with the protection requirements of EC Council Directive 89/336/EEC 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 B Information Technology Equipment according to CISPR 22 / European Standard EN 55022. The limits for Class B equipment were derived for typical residential environments to provide reasonable protection against interference with licensed communication devices.

Properly shielded and grounded cables and connectors (IBM part number 75G5958 or its equivalent) must be used in order to reduce the potential for causing interference to radio and TV communications and to other electrical or electronic equipment. Such cables and connectors are available from IBM authorized dealers. IBM cannot accept responsibility for an interference caused by using other than recommended cables and connectors.

**Terms and conditions for downloading and printing information**

Permissions for the use of the information you have selected for download are granted subject to the following terms and conditions and your indication of acceptance thereof.

**Personal Use:** You may reproduce this information for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of this information, or any portion thereof, without the express consent of the manufacturer.

**Commercial Use:** You may reproduce, distribute and display this information solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of this information, or reproduce, distribute or display this information or any portion thereof outside your enterprise, without the express consent of the manufacturer.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the information or any data, software or other intellectual property contained therein.

The manufacturer reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the information is detrimental to its interest or, as determined by the manufacturer, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations. THE MANUFACTURER MAKES NO GUARANTEE ABOUT THE CONTENT OF THIS INFORMATION. THE INFORMATION IS PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

All material copyrighted by IBM Corporation.

By downloading or printing information from this site, you have indicated your agreement with these terms and conditions.
Product recycling and disposal

This unit contains materials such as circuit boards, cables, electromagnetic compatibility gaskets and connectors which may contain lead and copper/beryllium alloys that require special handling and disposal at end of life. Before this unit is disposed of, these materials must be removed and recycled or discarded according to applicable regulations. IBM offers product-return programs in several countries. Information on product recycling offerings can be found on IBM’s Internet site at http://www.ibm.com/ibm/environment/products/prp.shtml.

IBM encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. IBM offers a variety of programs and services to assist equipment owners in recycling their IT products. Information on product recycling offerings can be found on IBM’s Internet site at http://www.ibm.com/ibm/environment/products/prp.shtml.

Battery return program

This product may contain sealed lead acid, nickel cadmium, nickel metal hydride, lithium, or lithium ion battery. Consult your user manual or service manual for specific battery information. The battery must be recycled or disposed of properly. Recycling facilities may not be available in your area. For information on disposal of batteries outside the United States, go to http://www.ibm.com/ibm/environment/products/batteryrecycle.shtml or contact your local waste disposal facility.

In the United States, IBM has established a return process for reuse, recycling, or proper disposal of used IBM sealed lead acid, nickel cadmium, nickel metal hydride, and other battery packs from IBM Equipment. For information on proper disposal of these batteries, contact IBM at 1-800-426-4333. Please have the IBM part number listed on the battery available prior to your call.

In the Netherlands, the following applies:

In Taiwan, the following applies. Please recycle batteries.

IBM Cryptographic Coprocessor Card Return Program

This machine may contain an optional feature, the cryptographic coprocessor card, which includes a polyurethane material that contains mercury. Follow local ordinances or regulations for disposal of this card. IBM has established a return program for certain IBM Cryptographic Coprocessor Cards. More information can be found at: http://www.ibm.com/ibm/environment/products/prp.shtml