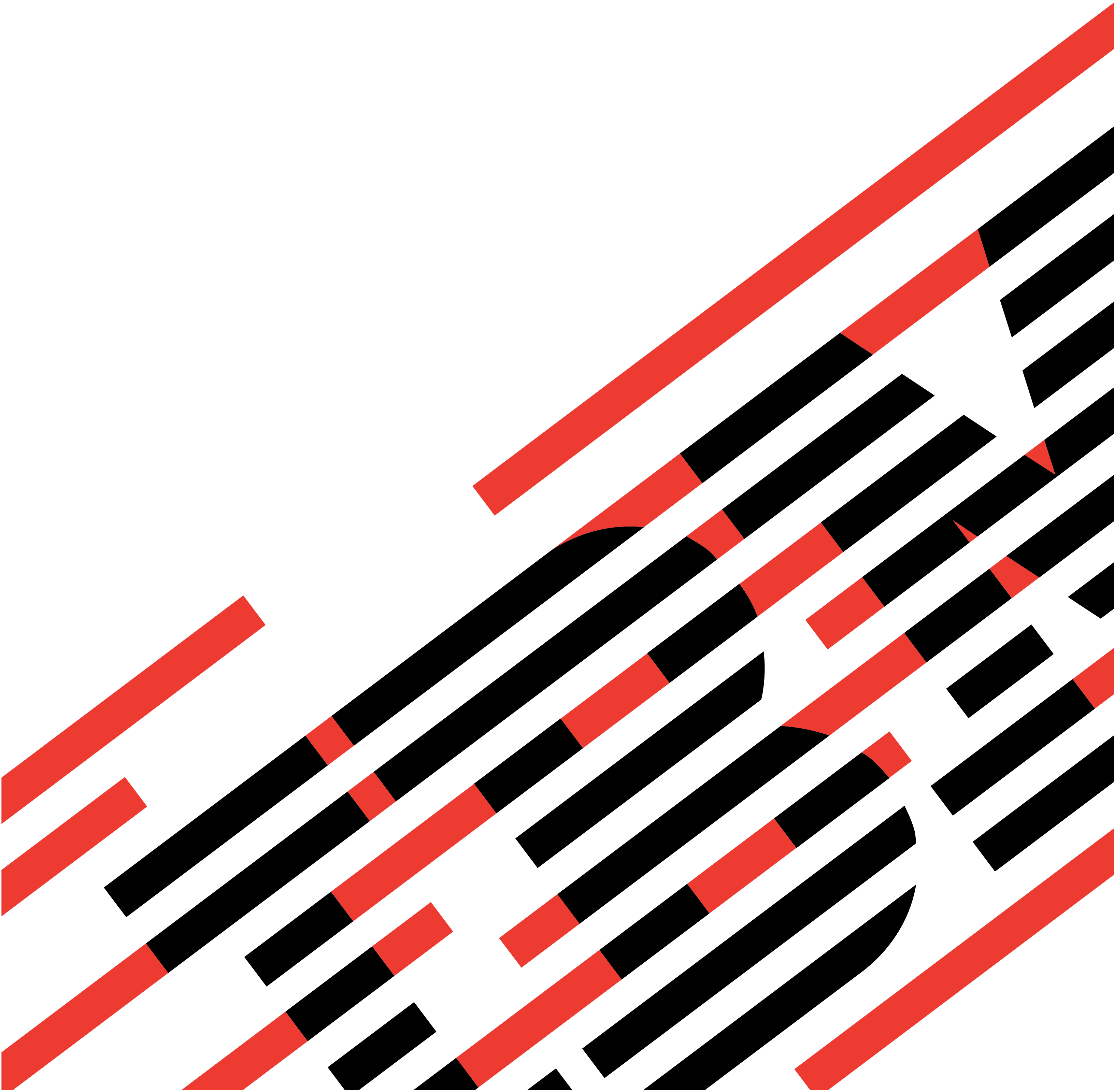
IBM

eserver

# Service and support



# Service and support

**Note**

Before using this information and the product it supports, be sure to read the information in "Notices," on page 99 and the manual *IBM eServer Safety Information*, G229-9054.

**Fourth Edition (December 2004)**

# Contents

# Service and support

Servers are equipped with tools to help you determine when you need to perform service or call for help. These servers can be enabled to automatically link to online support if a problem occurs. The information in this section helps you to understand the service and support options, and to plan for your service and support requirements.

Depending on the server model, many service tasks might be performed by customer personnel. The Troubleshooting information is available to help a server operator, or other customer personnel, to perform service tasks. If a problem occurs and a trained service person is required to perform diagnostics or other repair actions, the Authorized service provider information is available.

Customer service and support
Information to help you enable your server to monitor itself and to communicate information to your service or support provider.

Authorized service provider information
Information that is intended for use by authorized service providers to service and support your hardware.

## Customer service and support

The service and support environment of your server is enabled by built-in hardware and software. The service applications work together with the built-in hardware and software to provide automated service features and functions.

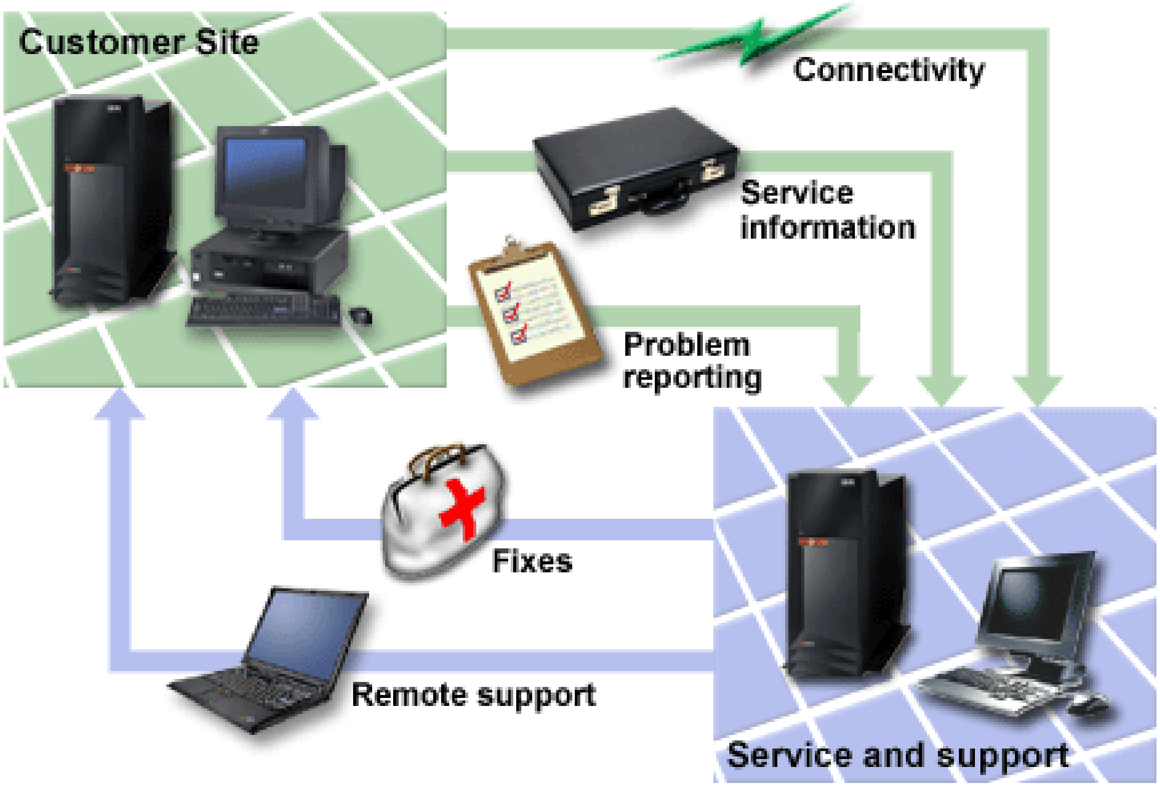
**Note:** If you need to perform manual problem analysis on your server, see Troubleshooting. The Troubleshooting topic helps you understand, isolate, and resolve problems. For example, if the system attention light is on, you can look up reference codes to understand what they mean and actions you can take to resolve them.

**Introduction to the service applications**

The service applications are tools that help monitor your server and connect your server to your service or support organization.

After your server is set up and connected to your service or support organization, the service applications enable service functions to occur automatically. The following applications are related to service and support for your server:
- Electronic Service Agent™
- Service Focal Point
- Remote Support Facility

The functions that the service tools enable are depicted in the following illustration. The service tools work together to help your server keep you informed of the status of issues that might occur, and to communicate information about those issues to your service or support organization.



The following topics provide more detailed information about various service or support environments and configurations:

**Printable PDF**
Learn how to print a PDF version of this topic, and how to save it to your workstation.

**Service and support overview**
Learn about the service options and the tools needed to support various operating environments.

**Scenarios: Service and support**
Learn from example scenarios how to connect and configure your server to contact service and support personnel.

**Setting up your service environment**
Learn how to set up and configure your server to work in your service environment.

**Customizing your service settings**
Learn about what to do when your service and support requirements change.

**Reporting problems**
Learn how to report problems when your server's service and support connections are not available.

**Getting fixes**
Learn about getting firmware, machine code, and operating system fixes.

**Enabling remote support**
Learn how to set up your server so that you can enable remote support centers to connect and manage your server.

**Related information about service and support**
View and print information related to the Customer service and support topic collection.

## What's new

Enhancements to the Customer service and support topic include the following:

**Enhanced information about fixes**

Getting fixes provides enhanced information about fixes for your HMC machine code, server firmware, and operating system. Use the scenarios to learn how to download and install your server firmware fixes either through the HMC or through the operating system, depending on your service environment. Learn about tasks you can perform to manage your server firmware fixes.

**AIX and Linux are now available**

New scenarios demonstrate how to set up your server running AIX or Linux to connect to the service provider.

**Concurrent firmware feature**

New feature allows server and power subsystem firmware that is available at the selected repository to be retrieved, installed, and activated concurrently.

## Printable PDF

To view or download the PDF version of this document, select Customer service and support (about 1500 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 want 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 (http://www.adobe.com/products/acrobat/readstep.html) .

## Service and support overview

Traditionally, service and support has been thought of as a set of resources you call on when you have a problem or failure. The service and support tools described in this section can help you to keep your server up and running and also save you time.

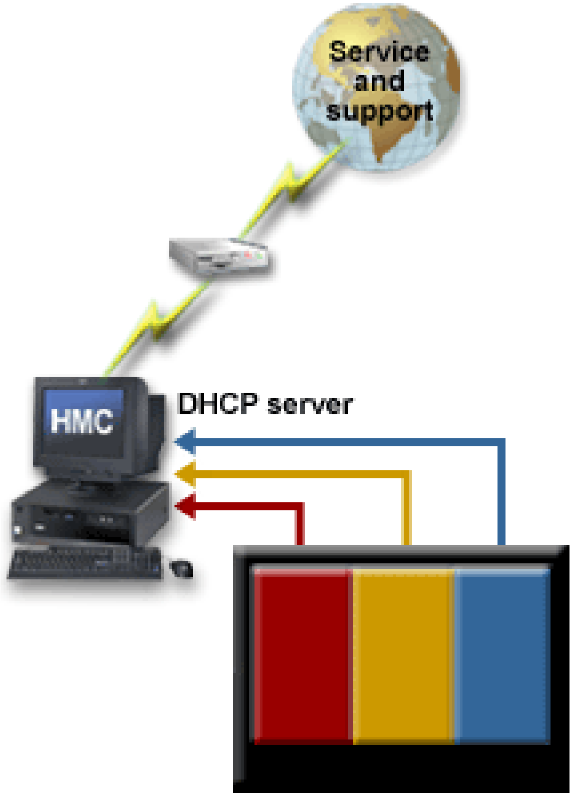
Some of the capabilities that are provided by the service and support applications are:

- Monitoring servers
- Monitoring logical partitions
- Communicating with your service and support organization
- Getting fixes
- Enabling remote support

There are several elements of service and support, including the following service applications:

- Electronic Service Agent
- Service Focal Point
- Remote Support Facility

These service applications (or tools) can be used on your server to enable your service environment. As depicted in the following illustration, if you are using logical partitions, the service tools run in each logical partition and work with the Hardware Management Console (HMC) as part of the service environment.



In this illustration there are three logical partitions running on a server. Each logical partition communicates with the HMC. The HMC then connects to your service or support organization. The hardware can be configured to automatically handle these tasks for you. If the applications are enabled, your server can report a problem to the service or support organization without your intervention. If a service person is needed, you can arrange to have the service performed and to recover from a problem as quickly as possible.

This topic describes the various aspects of service and support that you can use to ensure that your server and applications are ready when you need them. For details about the elements of service, service applications, and how these tools work together, see the following topics:

**Elements of your service environment**
Learn about the elements that are needed for your service environment.

**Introduction to the service applications**
Learn about the applications that are designed to help you manage your service and support requirements.

**Map of service applications and functions**
Learn about how each element of your service environment fits together to provide your service solution.

## Elements of your service environment

The following elements are necessary to provide quick access to service and support:

**Connectivity**
Learn about the advantages of connecting your server directly to your support and service providers.

**Service information**
Learn about how keeping your service or support organization up to date with your service information helps when service or support is needed.

**Electronic problem reporting**
Learn about how electronic problem reporting allows you to automatically notify your service and support people about any problems that might occur.

**Fixes**
Learn about ongoing fix support for your server or HMC and how to obtain software and firmware fixes.

**Remote support**
Learn about methods of connecting to your service and support organization to enable remote support.

**Connectivity:** Connectivity from your server or HMC to your service or support organization helps accelerate the process required to maintain your server. The connection method you choose depends on several factors, such as:

- How is your server hardware, software, and network configured?
- Do you have high-speed Internet access, or do you connect to the Internet using a modem?
- Do you have security requirements that you should consider?
- Are you planning to connect to your service or support organization using a console (such as an HMC) or through the server without an HMC?

The service tools that are provided with your server allow connection to service and support systems with or without the use of an HMC. Remote support is also an option for you to consider.

For more information about remote support, see the following:

- Remote Support Facility
- Scenarios: Service and support

**Service information:** Each operating system environment has tools that can help you keep service information about your server. This information can help your authorized service provider or your support organization provide better service or support. You can enable your server to automatically connect to your authorized service provider or support organization.

If you have i5/OS, you can use iSeries™ Navigator to collect and manage various types of service information on a regular basis, and store the information on a designated central system. For example, you can collect the information for users and groups, fixes, system values, hardware resources, software resources, service attributes, contact information, or network attributes. You might have other applications installed that allow you to collect lists of other types of resources.

The server has vital product data (VPD) that is stored internally. The VPD consists of information such as how much memory is installed, and how many processors are installed. These records provide valuable information which can be used by remote service and support personnel so that they can help you keep the firmware and software on your server up to date.

You can share this information with your service and support organization through Electronic Service Agent, which enables your service and support organization to help you identify problems and troubleshoot them more quickly.

The following list provides links to information about the tools used to gather the service information and send it to your service or support personnel:

Electronic Service Agent

Configuring Electronic Service Agent on your HMC

Customizing your service settings

**Electronic problem reporting:** Your server can help you isolate the cause of most hardware and software problems. If a problem occurs your server communicates with your supporting service organization to help isolate the cause of the problem. Depending on the problem, any one of the following actions can result:

- A fix can be sent to you, if one has already been identified.
- A hardware part can be sent to you for you to install, if appropriate.
- Your service or support organization can call you to gather more information and help you perform further problem analysis.
- A service person can be dispatched to your location.

For more information about using the service tools, use the following links:

- Electronic Service Agent
  Learn how Electronic Service Agent can help you maintain your system.
- Service Focal Point
  Learn how Service Focal Point helps isolate problems that affect multiple logical partitions.
- Setting up your service environment
  Learn about the process of setting up the service tools. This includes Electronic Service Agent and Service Focal Point, for example.
- Reporting problems
  Learn about how to report problems to your service and support provider when the automatic reporting process is not available.
- Troubleshooting topic
  Learn about troubleshooting and reporting problems that are not reported electronically.

**Fixes:** Periodically, a problem might be discovered in your server's software or firmware. If a problem is discovered in your software, a software fix, sometimes referred to as a *program temporary fix* (PTF), is distributed. If a problem is discovered in the firmware, the fix might be released as a PTF or as a firmware fix, depending on the server type and model.

Fixes play an important part in your server's maintenance strategy. They give you a chance to reduce system downtime, add functionality, or provide optimal availability. It is important that you develop a fix-management strategy to help you keep track of code fixes that are available for your software and firmware.

The Getting fixes topic provides more detail about how to download and install various types of fixes.

**Remote support:** In some cases, your service and support personnel can connect directly to your server to try to determine the source of a problem. Your service and support organization can use any of the following methods to connect to your server after you have enabled the connection:

- Virtual private networking (VPN): Uses several important TCP/IP protocols to protect data traffic.
- Point-to-Point Protocol (PPP): This Internet standard for transmitting data over serial lines is the most widely used connection protocol among Internet Service Providers (ISPs). PPP allows individual computers to access networks, which in turn provide access to the Internet.
- Systems Network Architecture (SNA): In service and support organization networks, SNA is the layered logical structure, formats, protocols, and operational sequences that are used for transmitting information units through networks. SNA also controls the configuration and operation of networks. APPC, APPN, and HPR are some examples of the protocols included within SNA. These protocols can be used to connect your server with other servers, to connect remote controllers, and to maintain a high level of security on your system.
- RSF: Provides support personnel with diagnostic access to the licensed internal code of the server.

  If a support person determines that this method is the best way to diagnose and fix your problem, you will be given detailed information about how to enable the connection.

For more information about the Remote Support Facility, use the following links:

- Remote Support Facility
  Learn how the Remote Support Facility can help you in your service environment.
- Enabling remote support
  Learn how to enable your system to allow a support person to remotely perform tasks on your hardware.

For specific information on using remote support with i5/OS, see the following topic collections:

- Virtual private networking
- Start Remote Support (STRRMTSPT) command
- Remote Access Services: PPP connections

## Introduction to the service applications

The applications that are used to help service and support your hardware depend on your hardware configuration and your operating environment. If your server is managed with a Hardware Management Console (HMC), the way in which you use the service applications differs from a server that does not have an HMC. Your specific configuration can be determined ahead of time, and then as you install your server and operating system environment, you can set up your service applications to best suit your needs.

The tools in the following list each provide features that help you maintain your server. Click on the following links to learn about the tools.

**Electronic Service Agent**
Learn more about the Electronic Service Agent application.

**Remote Support Facility**
Learn more about using the Remote Support Facility.

**Service Focal Point**
Learn about the Service Focal Point application.

**Electronic Service Agent:** The Electronic Service Agent application monitors your servers. If Electronic Service Agent is installed on your HMC, the HMC can monitor all the managed servers. If a problem occurs and the application is enabled, Electronic Service Agent can report the problem to your service and support organization. If your server is partitioned, Electronic Service Agent, together with the Service Focal Point application, reports serviceable events and associated data collected by Service Focal Point to your service and support organization.

**Note:** Serviceable events on the HMC typically consist of problems related to the server firmware and hardware, or problems related to Linux™ or AIX® hardware. Problems related to i5/OS™ are not typically reported through the HMC as serviceable events; i5/OS problems are reported through the logical partition and then sent to the service provider using the appropriate service connection.

The Electronic Service Agent Gateway maintains the database for all the Electronic Service Agent data and events that are sent to your service and support organization, including any Electronic Service Agent data from other client HMCs in your network.

You can enable Electronic Service Agent to perform the following tasks:

- Report problems automatically; service calls are placed without intervention.
- Automatically send service information to your service and support organization.
- Automatically receive error notification either from Service Focal Point or from the operating system running in a full system partition profile.
- Support a networked environment with a minimum number of telephone lines for modems.

For a more detailed description of configuring and using Electronic Service Agent, see Using the Guided Setup wizard to set up your HMC.

Electronic Service Agent can also be used on the servers.

To find out how Electronic Service Agent fits into your service environment, see Map of service applications and functions.

**Remote Support Facility:** The Remote Support Facility is an application that runs on the HMC and enables the HMC to call out to a service or support facility. The connection between the HMC and the remote facility can be used to:

- Allow automatic problem reporting to your service and support organization
- Allow remote support center personnel to directly access your server in the event of a problem

To find out how the Remote Support Facility fits into your service environment, see the Map of service applications and functions.

**Service Focal Point:** The Service Focal Point application is used to help service personnel to diagnose and repair problems on partitioned systems. Service personnel use the HMC as the starting point for all hardware service issues. The HMC gathers various hardware system-management issues at one control point, allowing service personnel to use the Service Focal Point application to determine an appropriate hardware service strategy.

Traditional service strategies become more complicated in a logically partitioned environment. Each logical partition runs on its own, unaware that other logical partitions exist on the same system. If a shared resource such as a power supply has an error, the same error might be reported by each partition using the shared resource. The Service Focal Point application enables service personnel to avoid long lists of repetitive call-home information by recognizing that these errors repeat, and by filtering them into one serviceable event.

For more information about the Service Focal Point application, see the following information:

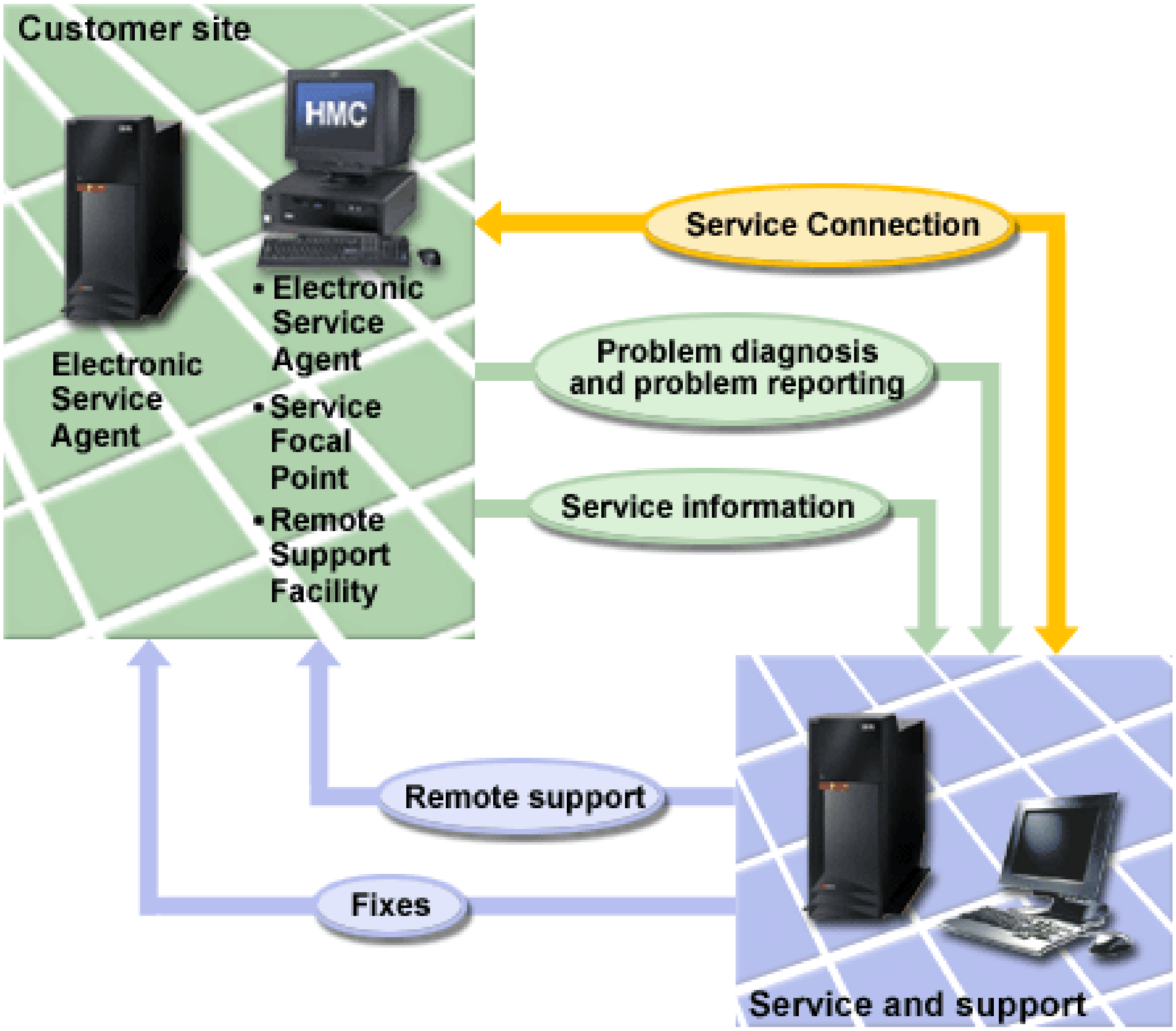
- Map of service applications and functions
  Find out how Service Focal Point fits into your service environment.

- Troubleshooting topic
  Find out how you can use Service Focal Point to troubleshoot problems.

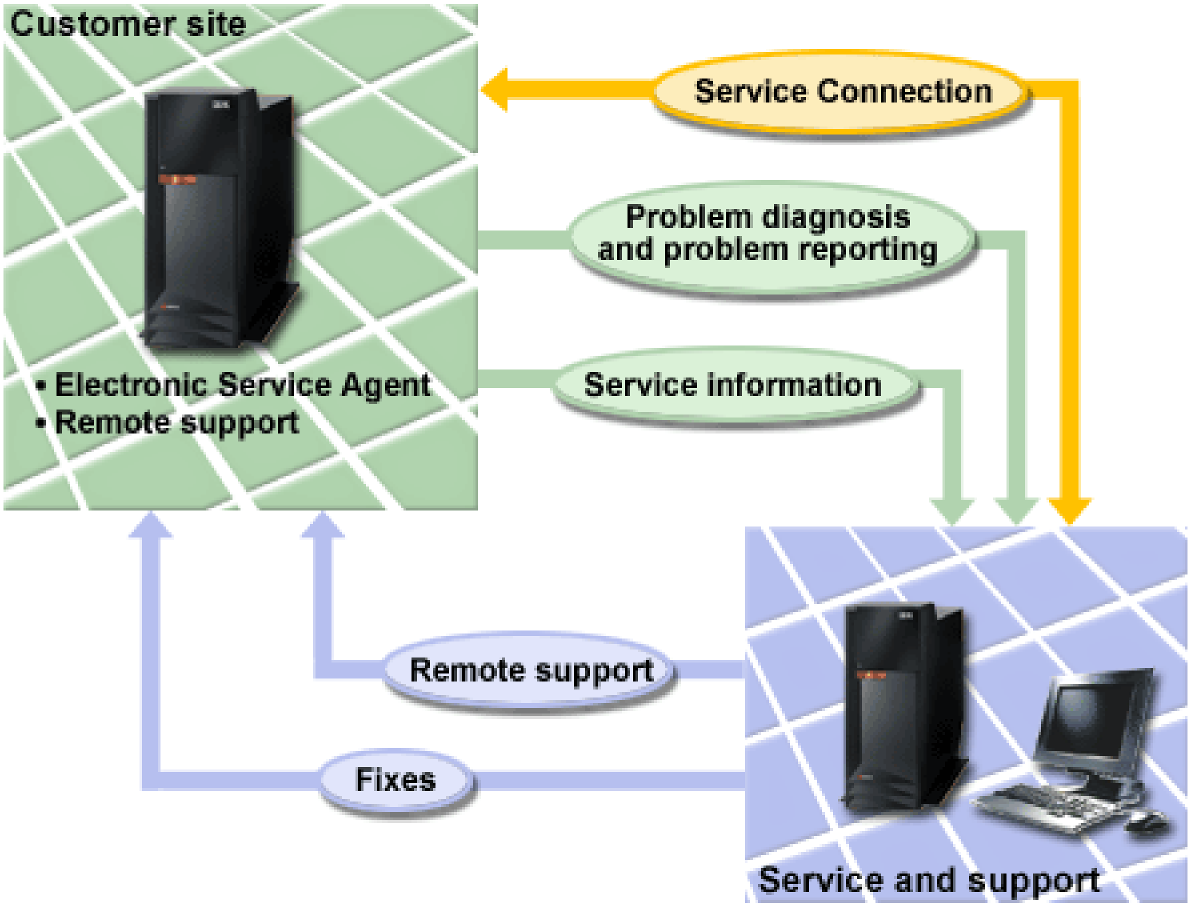
## Map of service applications and functions

Use the following illustrations to understand where the service applications run, whether on the server or the HMC, and to see the functions that occur within the service environment. The first illustration shows the HMC with its HMC-managed server. The second illustration shows a server with no HMC.

The following illustration shows a server and an HMC at the customer site that are connected to the service and support organization. Service applications that run on the server and HMC appear beneath each machine in the illustration. These applications perform the service-related functions that appear on the directional arrows that run between the customer site and the service and support organization. The service applications enable the server and HMC to report problems and service information to the service provider, and they enable the service and support organization to provide remote support and to send fixes to the customer site.



The following illustration shows a server at the customer site. The server is connected to the service and support organization. Service applications that run on the server appear beneath the server in the illustration. These applications perform the service-related functions that appear on the directional arrows between the customer site and the service and support organization. The service applications enable the server to report problems and send service information to the service provider, and they enable the service and support organization to provide remote support and to send fixes to the customer site.



## Scenarios: Service and support

These scenarios demonstrate several ways you can connect your server to your service provider for service and support. A server with numerous partitions, different operating systems, and an HMC has requirements that determine how to best use the service tools, while a server that does not have an HMC has different requirements. If you manage your server with an HMC, you can use the Guided Setup wizard to install your service tools. If you do not have an HMC, you can set up your service tools manually.

Compare the following scenarios to your own server environment, and set up your server to best meet your service and support requirements.

**Scenarios: AIX**
If you are running the AIX operating system, follow this link to find the most common service scenarios for AIX.

**Scenarios: i5/OS**
If you are running the i5/OS operating system, follow this link to find the most common service scenarios for i5/OS.

**Scenarios: Linux**
If you are running the Linux operating system, follow this link to find the most common service scenarios for Linux.

## Scenarios: AIX

If you are running AIX in a full system partition profile on a single server, or in multiple partitions on multiple servers, you can set up your server to contact your service and support organization. These scenarios demonstrate how you can connect your AIX logical partition to your service provider. Review the following scenarios to become familiar with the technical and configuration details. Find the connectivity method that works best with your hardware.

**Scenario: Multiple AIX logical partitions with an HMC**
Learn how to connect your logical partitions to enable service features on your server and your HMC.

**Scenario: AIX without an HMC**
Learn how to connect one server or multiple servers in a configuration that enables service features.

### Scenario: Multiple AIX logical partitions with an HMC: Situation

Suppose that you are responsible for maintaining the servers for MyCompany. As part of providing this support, you must establish the connections within your network and between MyCompany and your service provider that are needed to access service and support resources. You are using an HMC to manage your server and you have four logical partitions.

**Objectives**

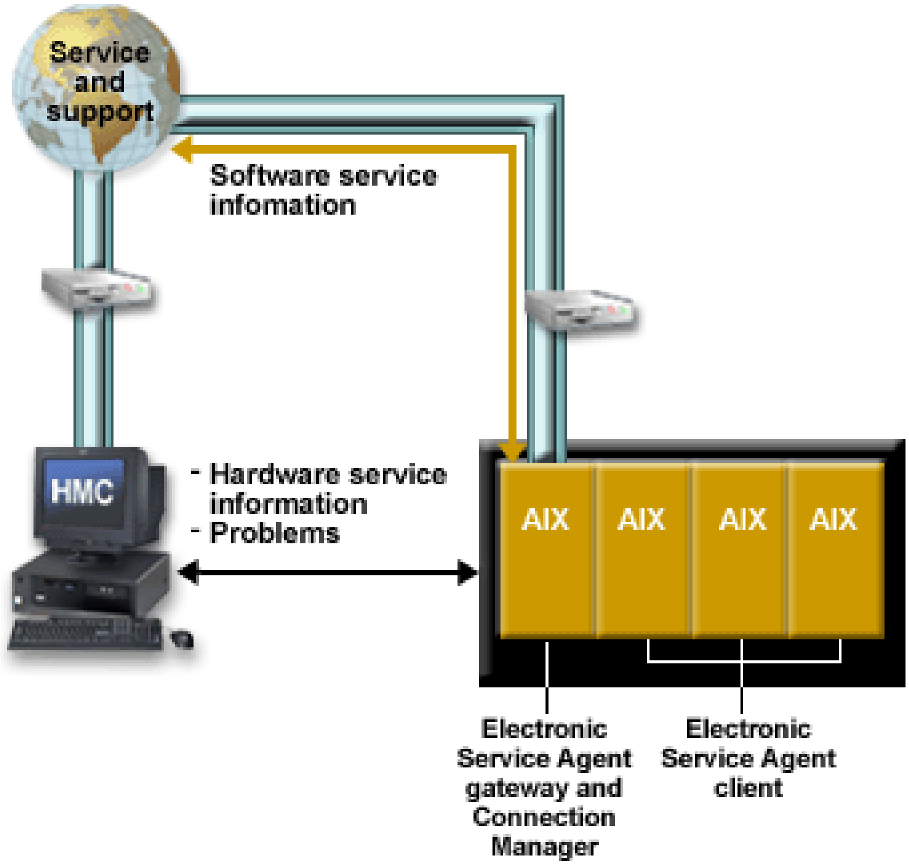
In this scenario, MyCompany wants to ensure that its service organization can support the MyCompany server when requested by the company's network administrator. The objectives of this scenario are as follows:

- To set up the HMC to connect to the service provider
- To set up the modem on a logical partition to connect to the service provider

  **Note:** Alternatively, you can use an Internet connection instead of the modem to connect to the service provider.
- To configure Electronic Service Agent on the logical partition that has a modem to be the Service Agent gateway server
- To configure Electronic Service Agent on other logical partitions to be Service Agent clients and to communicate with the Service Agent gateway server

**Details**

The following figure illustrates the flow of service information and problems through the service connection to the service organization.


Service and support
Software service infomation
HMC
- Hardware service information
- Problems
AIX
AIX
AIX
AIX
Electronic Service Agent gateway and Connection Manager
Electronic Service Agent client

The figure illustrates the following points relevant to this scenario:

- The HMC setup is complete.
- The HMC is set up with a modem that connects to the service provider.
- The server has four AIX logical partitions.
- Electronic Service Agent is configured on the HMC and on the logical partitions.
- The HMC is set up to use Electronic Service Agent to call out to the appropriate service and support organization.
- A logical partition is set up to use Electronic Service Agent to contact the software service support organization.
- The Service Agent gateway server and Connection Manager are set up on a logical partition with a modem that connects to the service provider.
- The Service Agent clients are set up on three other logical partitions.
- Hardware service information and problems flow from each logical partition to the service provider using the modem on the HMC, as follows:
  AIX partition > HMC > Service and support
- Software service information flows from each logical partition to the service provider using the modem on the server, as follows:
  AIX partitions (Service Agent clients) > AIX partition (Service Agent gateway server) > Service and support

**Prerequisites and assumptions**

Successful implementation of this scenario requires that the following prerequisites and assumptions are met:

- All necessary hardware planning and setup are complete.
- The server has been partitioned.
- All system requirements, including operating system and software installation, have been met.

**Configuration steps**

You must complete the following tasks:

1. Set up the HMC to connect to the service provider. You can use either of the following methods to set up the HMC:
   - Guided Setup wizard: (Recommended method for initial setup)
     You typically use the Guided Setup wizard when you first set up your server. If you used the Guided Setup wizard to set up both your HMC and your service connections when you first set up your server, go to Step 2.

     The Guided Setup wizard is a tool on the HMC designed to set up the HMC. The wizard guides you through the steps required for setting up the HMC, including the steps for setting up service connectivity from the HMC to the service provider.
   - Manual setup:
     Use this method to create your service connections if you set up your HMC prior to performing this scenario but you did not set up your service connections at that time.

     The following steps are required to set up service connectivity from the HMC to the service provider.

     **Note:** This set of steps is a subset of the larger group of tasks provided by the HMC Guided Setup wizard.

     a. Set up networking for your service environment.
        Configure network settings to enable the HMC and your partitions to communicate with one another over a private or open network.
     b. Choose the connection method.
        Configure your HMC to connect to your service provider using the modem and telephone line.
     c. Specify your company's contact and account information.
        Specify the information that is used when the HMC communicates with the service provider for service and software fixes.
     d. Configure the Electronic Service Agent on your HMC.
        Specify the information required to configure Electronic Service Agent on the HMC.
     e. Specify options for connection monitoring.
        Specify the options that enable Electronic Service Agent and Service Focal Point to perform service tasks.
2. Install the operating system on your logical partitions.
3. Set up your AIX server to connect to the service provider.
   Specify the information required to configure Electronic Service Agent in a logical partition to enable that partition to connect to a software service support organization.
4. Test your connection to the service provider.
   Verify that the connection to the service provider is set up correctly and that information is being transmitted correctly.

**Scenario: AIX without an HMC: Situation**

Suppose that you are responsible for maintaining the servers for ACompany. As part of providing this support, you must establish the connections within your network and between ACompany and your service provider. You are using a modem that is attached to one of your servers to communicate with your service provider.

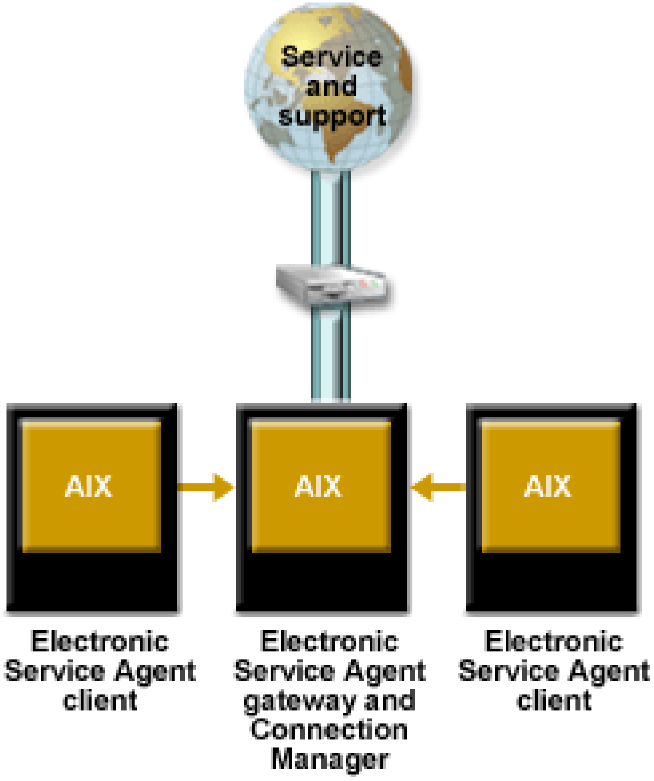
**Objectives**

In this scenario, ACompany wants to ensure that its servers are connected to its service provider so that support is available to the company's network administrator. The objectives of this scenario are as follows:

- To configure Electronic Service Agent on the server that has a modem for dial-up connection to the service provider

  **Note:** Alternatively, you can use an Internet connection instead of the modem to connect to the service provider.
- To configure Electronic Service Agent on the other client servers to communicate with the server that has the modem

The following figure illustrates the flow of service information and problems through the service connection from the servers to the service provider.


Service and support
AIX
AIX
AIX
Electronic Service Agent client
Electronic Service Agent gateway and Connection Manager
Electronic Service Agent client

The figure illustrates the following points relevant to this scenario:

- The Service Agent gateway server and Connection Manager are set up on the server with a modem that connects to the service provider.
- The Service Agent clients are set up on the other servers.
- Service information and problems flow from each client to the service provider using the modem on the server, as follows:
  AIX servers (Service Agent clients) > AIX server (Service Agent gateway server) > Service and support.

**Prerequisites and assumptions**

Successful implementation of this scenario requires that the following prerequisites and assumptions are met:

- All necessary hardware planning and setup are complete.
- All system requirements, including operating system and software installation, have been met.

**Configuration steps**

You must complete the following tasks:

1. Install the operating system on your servers.
2. Set up your AIX servers to connect to the service provider.
   Specify the information required to configure the Electronic Service Agent on the gateway server and the client servers.
3. Test your connection to the service provider
   Verify that the connection to the service provider is set up correctly and that information is being transmitted correctly.

## Scenarios: i5/OS

These scenarios demonstrate several ways you can connect your i5/OS logical partition to your service provider for service and support. Review the following scenarios to become familiar with the technical and configuration details. Find the connectivity method that works best with the hardware you use.

**Scenario: Multiple i5/OS logical partitions using VPN on an i5/OS logical partition**
This scenario demonstrates how to configure multiple logical partitions to connect to your service provider through a VPN connection on an i5/OS logical partition.

**Scenario: Multiple i5/OS logical partitions using the HMC modem**
This scenario demonstrates how to configure multiple logical partitions to connect to your service provider through the modem on the HMC.

**Scenario: Multiple i5/OS logical partitions using the modem on an i5/OS logical partition**
This scenario demonstrates how to configure multiple logical partitions to connect to your service provider through the modem on an i5/OS logical partition.

**Scenario: Multiple i5/OS logical partitions using the HMC modem and the modem on an i5/OS logical partition**
This scenario demonstrates how to configure multiple i5/OS logical partitions to connect to the service provider through the modem on the i5/OS logical partition and to enable the HMC to connect to the service provider through its own modem. In the event the HMC modem is busy or unavailable, the HMC can use the modem on the i5/OS logical partition to connect to the service provider.

**Scenario: i5/OS without an HMC using VPN**
This scenario demonstrates how to configure i5/OS to use VPN to connect to your service provider when you do not use an HMC to manage your system.

**Scenario: Multiple i5/OS logical partitions using VPN on an i5/OS logical partition: Situation**

Suppose that you are responsible for maintaining the servers for MyCompany, a manufacturing company. As part of providing this support, you must establish the connections within your network and between MyCompany and your service provider that are needed to access service and support resources. You are using an HMC to manage your server, and your server is divided into multiple logical partitions running multiple operating systems. Only one of your i5/OS logical partitions has connectivity to the Internet. For security reasons, you keep each of the other logical partitions on a separate, private network.

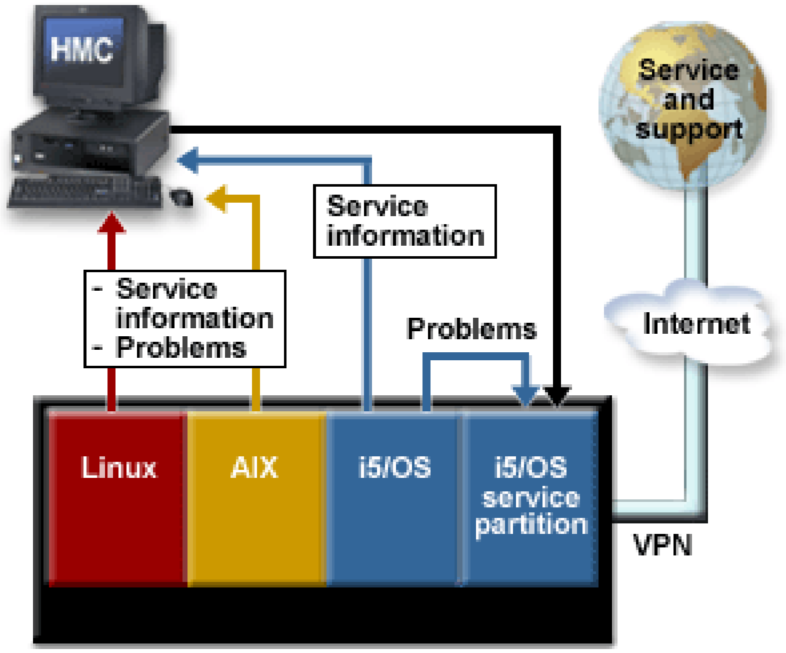
**Objectives**

In this scenario, MyCompany wants to ensure that its service provider can support the MyCompany server when requested by the company's network administrator. The objectives of this scenario are as follows:

- To set up the HMC to connect to the service provider for service through the VPN connection on the i5/OS partition
- To create a VPN connection from the i5/OS logical partition that has connectivity to the Internet
- To enable the other logical partitions to connect to the logical partition that has connectivity to the Internet

**Details**

The following figure illustrates the flow of service information and problems through the service connection to the service provider.



The figure illustrates the following points relevant to this scenario:

- The HMC setup is complete.
- The server has four logical partitions with the following operating systems installed:
  - Linux
  - AIX
  - i5/OS
  - i5/OS (This is the service partition)
- VPN is configured on the service partition and connects to the service provider.
- Service information and problems flow from each logical partition to the service provider using a VPN connection, as follows:
  - Linux logical partition > HMC > i5/OS service partition > Service and support
  - AIX logical partition > HMC > i5/OS service partition > Service and support
  - i5/OS logical partition > HMC (for service information) > i5/OS service partition > Service and support
  - i5/OS logical partition > i5/OS service partition (for problems) > Service and support
  - i5/OS service partition > Service and support

**Prerequisites and assumptions**

Successful implementation of this scenario requires that the following prerequisites and assumptions are met:

- All necessary hardware planning and setup are complete.
- The system has been partitioned.

Additional prerequisites and assumptions are noted in the appropriate places within the configuration tasks.

**Configuration steps**

You must complete the following tasks:

1. Set up the HMC to connect to the service provider for service and support. You can use either of the following methods to set up the HMC:
   - Guided Setup wizard: (Recommended method for initial setup)
     You typically use the Guided Setup wizard when you first set up your HMC and server. If you used the Guided Setup wizard to set up both your HMC and your service connections when you first set up your server, go to Step 2.

     The Guided Setup wizard is a tool on the HMC designed to set up the HMC. The wizard guides you through the steps required for setting up the HMC, including the steps for setting up service connectivity from the HMC to the service provider.
   - Manual setup:
     Use this method to create your service connections if you set up your HMC prior to performing this scenario but you did not set up your service connections at that time.

     The following steps are required to set up service connectivity from the HMC to the service provider.

     **Note:** This set of steps is a subset of the larger group of tasks provided by the Guided Setup wizard.

     a. Set up networking for your service environment.
        Configure network settings to enable the HMC and your logical partitions to communicate with one another over a private or open network.
     b. Choose the connection method.
        Configure your HMC to connect to your service provider using the appropriate method. For this scenario, select **Connecting through other systems or logical partitions** when you choose the connection method.
     c. Specify your company's contact and account information.
        Specify the information that is used when the HMC communicates with the service provider for service and software fixes.
     d. Configure Electronic Service Agent on your HMC.
        Specify the information required to configure Electronic Service Agent on the HMC.
     e. Specify options for connection monitoring.
        Specify the options that enable Electronic Service Agent and Service Focal Point to perform service tasks.
2. Install the operating systems on your logical partitions.
3. Set up your server to connect to your service provider.
   Create a VPN connection from the i5/OS logical partitions.
4. Test your connection to your service provider.
   Verify that the connection to your service provider is set up correctly and that information is being transmitted correctly.

**Scenario: Multiple i5/OS logical partitions using the HMC modem: Situation**

Suppose that you are responsible for maintaining the servers for MyCompany, a manufacturing company. As part of providing this support, you must establish the connections within your network and between MyCompany and your service provider that are needed to access service and support resources. You are using an HMC to manage your server, and your server is divided into multiple logical partitions. You want to enable your server to use the modem on the HMC for service and support.

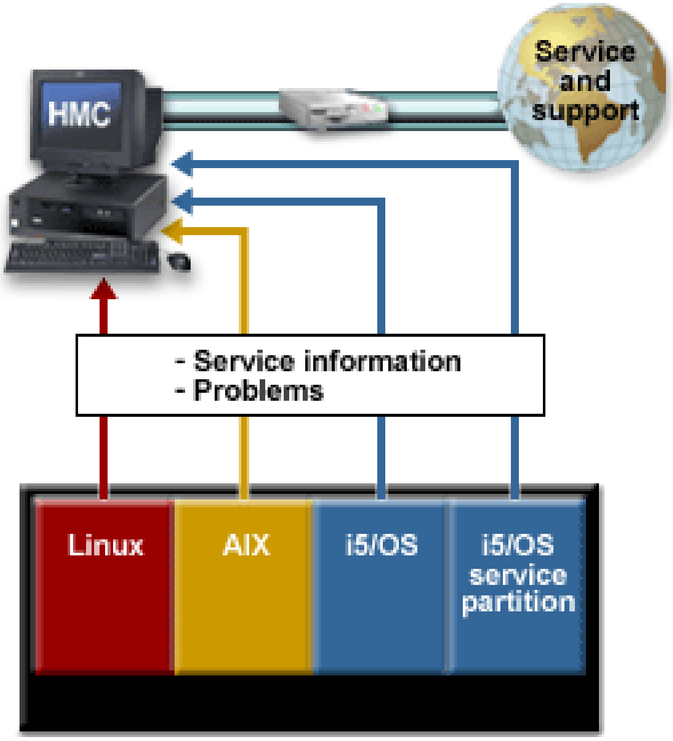
**Objectives**

In this scenario, MyCompany wants to ensure that its service provider can support the MyCompany server when support is requested by the company's network administrator. The objectives of this scenario are as follows:

- To set up the HMC to connect to the service provider for service
- To configure each of the logical partitions to report through the modem on the HMC

**Details**

The following figure illustrates the flow of service information and problems through the service connection to the service provider.



The figure illustrates the following points relevant to this scenario:

- The HMC setup is complete.
- The server has four logical partitions with the following operating systems installed:
  - Linux
  - AIX
  - i5/OS
  - i5/OS (This is the service partition)
- The PPP connection is configured on the HMC and connects to the service provider.
- Service information and problems flow from each logical partition to the service provider using a PPP connection, as follows:

- – Linux logical partition > HMC > Service and support
- – AIX logical partition > HMC > Service and support
- – i5/OS logical partition > HMC > Service and support
- – i5/OS service partition > HMC > Service and support

**Prerequisites and assumptions**

Successful implementation of this scenario requires that the following prerequisites and assumptions are met:

- All necessary hardware planning and setup are complete.
- The system has been partitioned.

Additional prerequisites and assumptions are noted in the appropriate places within the configuration tasks.

**Configuration steps**

You must complete the following tasks:

1. Set up the HMC to connect to the service provider for service and support. You can use either of the following methods to set up the HMC:
   - Guided Setup wizard: (Recommended method for initial setup)
     You typically use the Guided Setup wizard when you first set up your HMC and server. If you used the Guided Setup wizard to set up both your HMC and your service connections when you first set up your server, go to Step 2.

     The Guided Setup wizard is a tool on the HMC designed to set up the HMC. The wizard guides you through the steps required for setting up the HMC, including the steps for setting up service connectivity from the HMC to the service provider.
   - Manual setup:
     Use this method to create your service connections if you set up your HMC prior to performing this scenario but you did not set up your service connections at that time.

     The following steps are required to set up service connectivity from the HMC to the service provider.

     **Note:** This set of steps is a subset of the larger group of tasks provided by the Guided Setup wizard.
     a. Set up networking for your service environment.
        Configure network settings to enable the HMC and your logical partitions to communicate with one another over a private or open network.
     b. Choose connection method.
        Configure your HMC to connect to your service provider using the appropriate method. For this scenario, select **Dial-up from the local HMC** when you choose the connection method.
     c. Specify your company's contact and account information.
        Specify the information that is used when the HMC communicates with the service provider for service and software fixes.
     d. Configure Electronic Service Agent on your HMC.
        Specify the information required to configure Electronic Service Agent on the HMC.
     e. Specify options for connection monitoring.
        Specify the options that enable Electronic Service Agent and Service Focal Point to perform service tasks.
2. Install the operating systems on your logical partitions.
3. Set up your server to connect to the service provider.
   Configure each logical partition to use the modem on the HMC to connect to the service provider.

4. Test your connection to the service provider.
   Verify that the connection to the service provider is set up correctly and that information is being transmitted correctly.

**Scenario: Multiple i5/OS logical partitions using the modem on an i5/OS logical partition: Situation**

Suppose that you are responsible for maintaining the servers for MyCompany, a manufacturing company. As part of providing this support, you must establish the connections within your network and between MyCompany and your service provider that are needed to access service and support resources. You are using an HMC to manage your server, and your server is divided into multiple logical partitions. One of your i5/OS logical partitions has a modem.

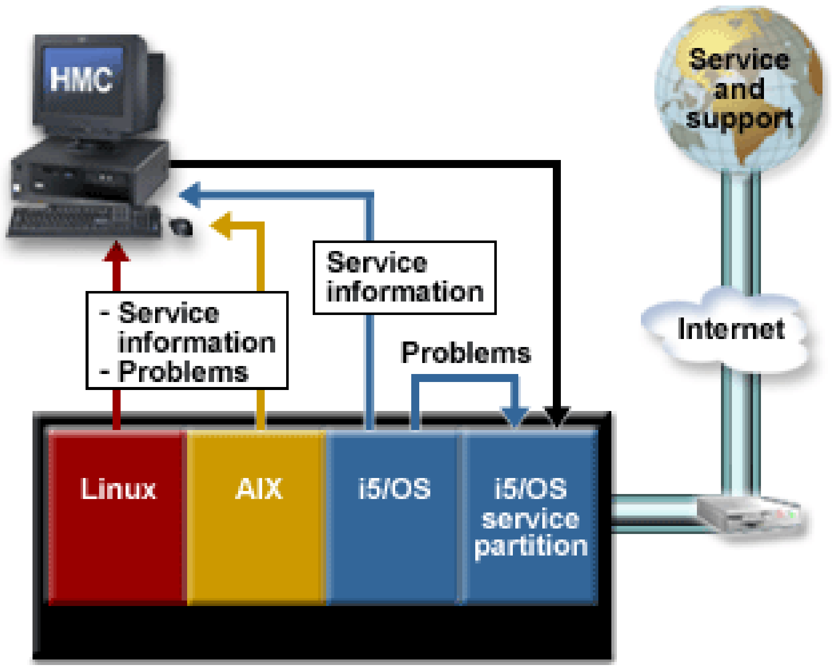
**Objectives**

In this scenario, MyCompany wants to ensure that its service provider can support the MyCompany server when support is requested by the company's network administrator. The objectives of this scenario are as follows:

- To set up the HMC to connect to the service provider for service
- To configure the i5/OS logical partition that has the modem for dial-up connection to the service provider
- To configure the other logical partitions to also use that modem

**Details**

The following figure illustrates the flow of information and problems through the service connection to the service provider.



The figure illustrates the following points relevant to this scenario.

- The HMC setup is complete.
- The server has four logical partitions with the following operating systems installed:

  - Linux
  - AIX
  - i5/OS
  - i5/OS (This is the service partition)
- The PPP connection is configured on the service partition and connects to the service provider.
- Service information and problems flow from each logical partition to the service provider using a PPP connection, as follows:
  - Linux logical partition > HMC > i5/OS service partition > Service and support
  - AIX logical partition > HMC > i5/OS service partition > Service and support
  - i5/OS logical partition > HMC (for service information) > i5/OS service partition > Service and support
  - i5/OS logical partition > i5/OS service partition (for problems) > Service and support
  - i5/OS service partition > Service and support

**Prerequisites and assumptions**

Successful implementation of this scenario requires that the following prerequisites and assumptions are met:

- All necessary hardware planning and setup are complete.
- The system has been partitioned.

Additional prerequisites and assumptions are noted in the appropriate places within the configuration tasks.

**Configuration steps**

You must complete the following tasks:

1. Set up the HMC to connect to the service provider for service and support:
   You can use either of the following methods to set up the HMC:
   - Guided Setup wizard: (Recommended method for initial setup)
     You typically use the Guided Setup wizard when you first set up your server. If you used the Guided Setup wizard to set up both your HMC and your service connections when you first set up your HMC and server, go to Step 2.

     The Guided Setup wizard is a tool on the HMC designed to set up the HMC. The wizard guides you through the steps required for setting up the HMC, including the steps for setting up service connectivity from the HMC to the service provider.
   - Manual setup:
     Use this method to create your service connections if you set up your HMC prior to performing this scenario but you did not set up your service connections at that time.

     The following steps are required to set up service connectivity from the HMC to the service provider.

     **Note:** This set of steps is a subset of the larger group of tasks provided by the Guided Setup wizard.

     a. Set up networking for your service environment.
        Configure network settings to enable the HMC and your logical partitions to communicate with one another over a private or open network.
     b. Choose connection method.
        Configure your HMC to connect to your service provider using the appropriate method. For this scenario, select **Connecting through other systems or logical partitions** when you choose the connection method.

   c. Specify your company's contact and account information.
      Specify the information that is used when the HMC communicates with the service provider for service and software fixes.
   d. Configure Electronic Service Agent on your HMC.
      Specify the information required to configure Electronic Service Agent on the HMC.
   e. Specify options for connection monitoring.
      Specify the options that enable Electronic Service Agent and Service Focal Point to perform service tasks.
2. Install the operating systems on your logical partitions.
3. Set up your server to connect to the service provider.
   Configure PPP connections from the i5/OS logical partitions.
4. Test your connection to the service provider.
   Verify that the connection to the service provider is set up correctly and that information is being transmitted correctly.

**Scenario: Multiple i5/OS logical partitions using the HMC modem and the modem on an i5/OS logical partition: Situation**

Suppose that you are responsible for maintaining the servers for MyCompany. As part of providing this support, you must establish the connections within your network and between MyCompany and your service provider that are needed to access service and support resources. You are using an HMC to manage your server, and your server is divided into multiple logical partitions running multiple operating systems. You want to enable the server to use the modem on the HMC or the modem on the server to connect to the service provider. In the event the HMC modem is busy or unavailable, the HMC can alternatively use the modem on the i5/OS logical partition to connect to the service provider.

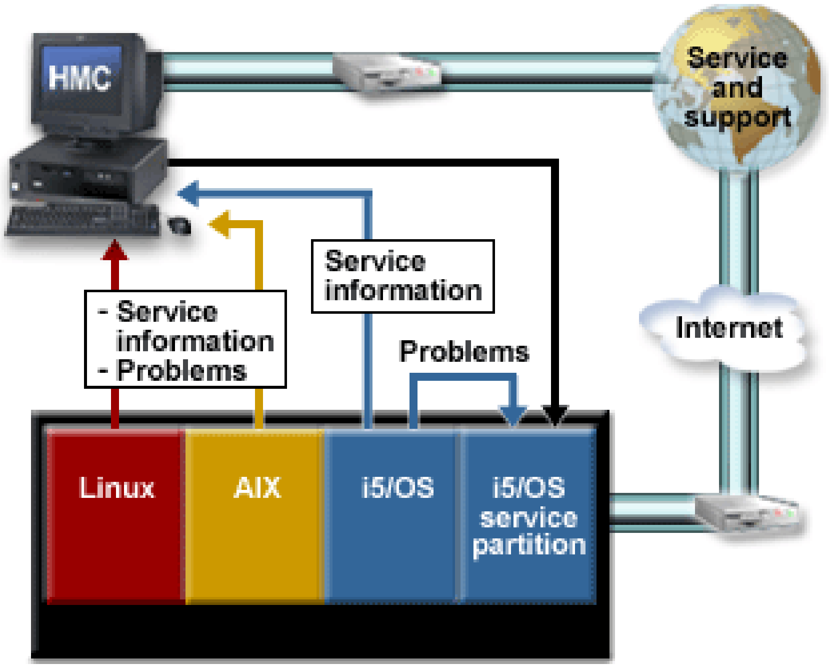
**Objectives**

In this scenario, MyCompany wants to ensure that its service provider can support the MyCompany server when requested by the company's network administrator. The objectives of this scenario are as follows:

- To set up the HMC to connect to the service provider for service and support
- To configure the i5/OS logical partition (non-service partition) to use the modem on the i5/OS service partition to report i5/OS problems to the service provider
- To configure the i5/OS logical partition that has the modem for dial-up connection to the service provider
- To enable the logical partitions running Linux, AIX, and i5/OS (non-service partition) to use the modem on the HMC to report service information, problems related to server hardware or firmware, and problems related to Linux and AIX to the service provider

**Details**

The following figure illustrates the flow of service information and problems through the service connection to the service provider.



The figure illustrates the following points relevant to this scenario:

- The HMC setup is complete.
- The server has four logical partitions with the following operating systems installed:
  - Linux
  - AIX
  - i5/OS
  - i5/OS (This is the service partition)
- The PPP connection is configured on the service partition and connects to the service provider.
- The logical partitions use either the modem on the HMC or the modem on the service partition to connect to the service provider.
- Service information and problems flow from each logical partition to the service provider using a modem connection, as follows:
  - Linux logical partition > HMC > Service and support
  - AIX logical partition > HMC > Service and support
  - i5/OS logical partition > HMC (for service information) > Service and support
  - i5/OS logical partition > i5/OS service partition (for i5/OS problems) > Service and support
  - i5/OS service partition > Service and support

**Note:** If the HMC modem is busy or unavailable, the HMC and logical partitions can alternatively use the modem on the service partition to send all service information and problems to the service provider.

**Prerequisites and assumptions**

Successful implementation of this scenario requires that the following prerequisites and assumptions are met:

- All necessary hardware planning and setup are complete.

- The system has been partitioned.

Additional prerequisites and assumptions are noted in the appropriate places within the configuration tasks.

**Configuration steps**

You must complete the following tasks:

1. Set up the HMC to connect to the service provider for service and support. You can use either of the following methods to set up the HMC:
   - Guided Setup wizard: (Recommended method for initial setup)
     You typically use the Guided Setup wizard when you first set up your HMC and server. If you used the Guided Setup wizard to set up both your HMC and your service connections when you first set up your server, go to Step 2.

     The Guided Setup wizard is a tool on the HMC designed to set up the HMC. The wizard guides you through the steps required for setting up the HMC, including the steps for setting up service connectivity from the HMC to the service provider.
   - Manual setup:
     Use this method to create your service connections if you set up your HMC prior to performing this scenario but you did not set up your service connections at that time.

     The following steps are required to set up service connectivity from the HMC to the service provider.

     **Note:** This set of steps is a subset of the larger group of tasks provided by the Guided Setup wizard.
     1. Set up networking for your service environment.
        Configure network settings to enable the HMC and your logical partitions to communicate with one another over a private or open network.
     2. Choose the connection methods.
        Configure your HMC to connect to your service provider using the appropriate methods. For this scenario, select both **Local Modem** and **Pass-through systems** when you choose the connection methods.
     3. Specify your company's contact and account information.
        Specify the information that is used when the HMC communicates with the service provider for service and software fixes.
     4. Configure Electronic Service Agent on your HMC.
        Specify the information required to configure Electronic Service Agent on the HMC.
     5. Specify options for connection monitoring.
        Specify the options that enable Electronic Service Agent and Service Focal Point to perform service tasks.
2. Install the operating systems on your logical partitions.
3. Set up your server to connect to your service provider.
   Configure PPP connections from the i5/OS logical partitions to use the modem on the service partition to report i5/OS problems to the service provider.
4. Test your connection to your service provider.
   Verify that the connection to your service provider is set up correctly and that information is being transmitted correctly.

**Scenario: i5/OS without an HMC using VPN: Situation**

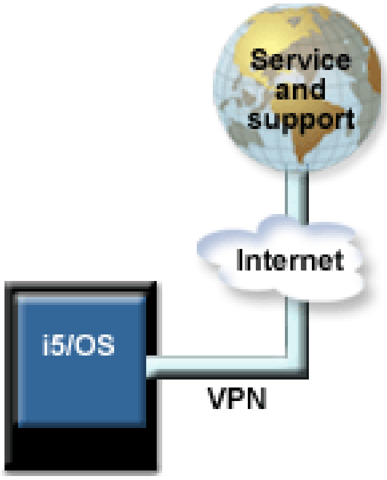
Suppose that you are responsible for maintaining the servers for MyCompany, a manufacturing company. As part of providing this support, you must establish the connections within your network and between MyCompany and your service provider that are needed to access service and support resources.

**Objectives**

In this scenario, MyCompany wants to ensure that the service provider can support the MyCompany server when support is requested by the company's network administrator. The objective of this scenario is to create a VPN connection from the server to the service provider.

**Details**

The following figure illustrates the flow of service information and problems through the service connection to the service provider.



The figure illustrates the following points relevant to this scenario:

- The server is in its manufacturing default configuration with i5/OS installed.
- The VPN connection is configured on the server and connects to the service provider.
- The service information and problems flow from the i5/OS logical partition to the service provider.

**Prerequisites and assumptions**

Successful implementation of this scenario requires that the following prerequisites and assumptions are met:

- All necessary hardware planning and setup are complete.
- Additional prerequisites and assumptions are noted in the appropriate places in the configuration tasks.

**Configuration steps**

You must complete the following tasks:

1. Install i5/OS on your logical partition.
2. Set up your server to connect to the service provider.
   Configure a VPN connection to the service provider from the server.
3. Test your connection to the service provider.
   Verify that the connection to the service provider is set up correctly and that information is being transmitted correctly.

## Scenario: Linux

This scenario demonstrates how to connect your Linux servers to your service provider for service and support. Review Scenario: Linux without an HMC to become familiar with the technical and configuration details.

### Scenario: Linux without an HMC: Situation

You are responsible for maintaining the servers for a manufacturing company. As part of providing this support, you must establish the necessary connections within your network and between your company and your service provider to access service and support resources.

#### Objectives

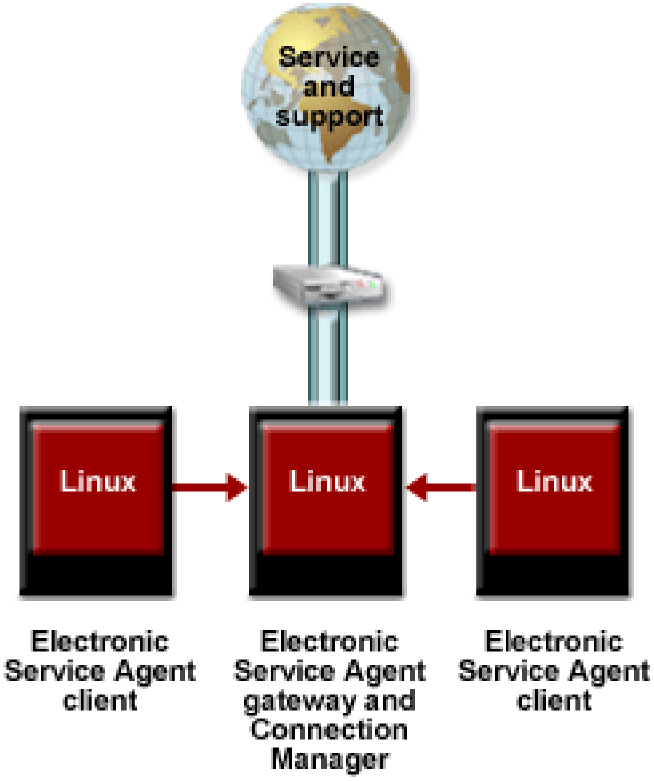
In this scenario, you want to ensure that your service provider can support your company's server when support is requested by the company's network administrator. The objectives of this scenario are as follows:

- To configure Electronic Service Agent on the server that has a modem connection to the service provider

  **Note:** Alternatively, you can use an Internet connection instead of the modem to connect to the service provider.
- To configure Electronic Service Agent on the other client servers to communicate with the server that has the modem

#### Details

The following figure illustrates the flow of service information and problems through the service connection to the service provider.


Service and support
Linux
Linux
Linux
Electronic Service Agent client
Electronic Service Agent gateway and Connection Manager
Electronic Service Agent client

The figure illustrates the following points relevant to this scenario.

- The Service Agent gateway server and Connection Manager are set up on the server with a modem that connects to the service provider.
- The Service Agent clients are set up on the other servers.

- Service information and problems flow from each client and gateway server to the service provider using the modem on the server, as follows:
  - Linux servers (Service Agent clients) > Linux server (Service Agent gateway server) > Service and support

**Prerequisites and assumptions**

Successful implementation of this scenario requires that the following prerequisites and assumptions are met:

- All necessary hardware planning and setup are complete.
- All system requirements, including operating system and software installation, have been met.
- Additional prerequisites and assumptions are noted in the appropriate places within the configuration tasks.

**Configuration steps**

You must complete the following tasks:

1. Set up your server to connect to your service provider.
   Configure a connection to your service provider from the server.
2. Test your connection to your service provider.
   Verify that the connection to your service provider is set up correctly and that information is being transmitted correctly.

## Setting up your service environment

This topic describes how to set up your server to use the service tools for your operating environment. If you need to set up your service processor to communicate with your service provider, the setup tasks for the service processor are also covered here.

The following links can help you get started for both Hardware Management Console (HMC) and non-HMC service setups:

**Using the Guided Setup wizard to set up your HMC**
This topic describes how to use the Guided Setup wizard to set up and configure the HMC and the service tools.

**Networking for your service environment**
This topic describes the networking options for your service environment.

**Setting up your HMC to connect to your service provider**
This topic has detailed information about setting up your HMC as the gateway to your service provider.

**Setting up your server to connect to your service provider**
This topic has detailed information about setting up your logical partition as the gateway to your service provider.

**Testing your connection to your service provider**
This topic has detailed information to help you test your connection to your service provider.

**Attention:**

During service activity, it is likely that the IBM® service representative will need to use one, or more, of the following:

- Hardware Management Console (HMC)
- System console
- PC capable of connecting to the Advanced System Management Interface (ASMI)

For this reason, IBM requires that the customer provide the following for the service representative's use:

- Provide a supported HMC, a system console, or a PC capable of connecting to the ASMI.
- Provide all current, supported software, loaded on the devices and properly configured, with current software fixes applied.
- Locate the consoles in the same room and within 8 meters (26 feet) of the system being serviced.
- Make sure the devices are connected to the system, operational, and communicating with the system prior to the arrival of the service representative.

Delays to service personnel that are caused by a failure to meet the requirements stated above, are billable at current hourly rates. Note: The HMC or system console might be capable of providing the required ASMI connection, if properly configured.

## Using the Guided Setup wizard to set up your HMC

The Guided Setup wizard steps you through the tasks that are required to set up your HMC, including the tasks that are required to set up your service environment. However, other tasks in the wizard are not specific to setting up service, including the following:

- Setting the date and time
- Changing passwords for the hscroot and root user IDs
- Creating user IDs and passwords for new users and setting their authorities
- Specifying network settings

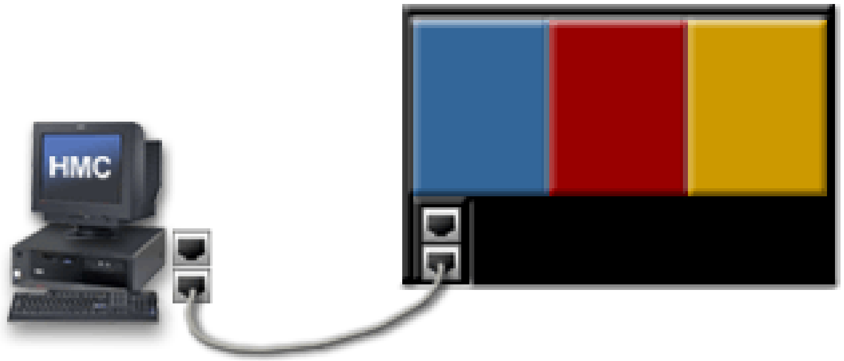
The Guided Setup wizard starts automatically the first time that you start your HMC. If the wizard does not start, see Accessing the Guided Setup wizard using the HMC interface.

## Networking for your service environment

The underlying framework of your service environment is networking. The following networking connections are required for you to be able to take advantage of electronic services such as reporting hardware problems and other server information and downloading fixes:

- Connecting to the service processor using a network connection

  The service processor is part of your platform hardware and monitors hardware attributes and conditions on your server. The service processor is controlled by server firmware and does not require an operating system to perform its tasks. You use the Advanced System Management Interface (ASMI) to change the settings of the service processor. The connection to the service processor is recommended for all servers, whether or not you have logical partitions. This connection is represented in the following illustration:



You can access the ASMI using your Hardware Management Console or any PC on your network that has a Web browser installed on it. For more information about how to connect to the service processor, see Accessing the Advanced System Management Interface.

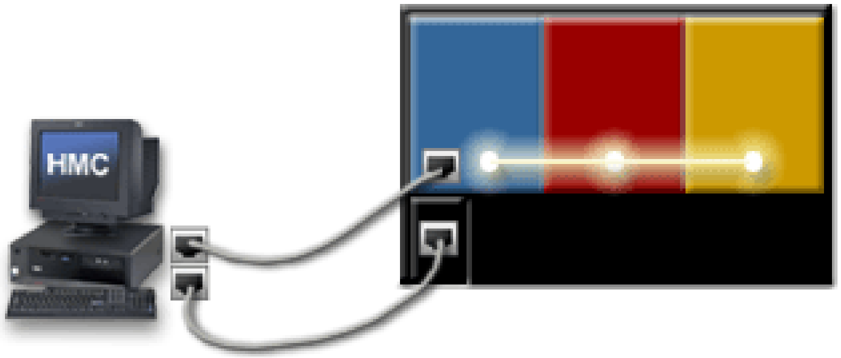
- Connection between the console and the server

  If your server is in its manufacturing default configuration, you will make this connection when you set up your server. For more information about the various consoles that are available and how to set them up, see Adding a console.

  If your server has multiple logical partitions, you must ensure that your HMC can communicate with each logical partition and that the logical partitions can communicate with each other. You will set up these connections as you create your logical partitions. You can use either of the following methods:

  **Note:** Both of the following networking methods require basic TCP/IP configuration on your partitions. Refer to your operating system documentation for instructions on how to configure TCP/IP.

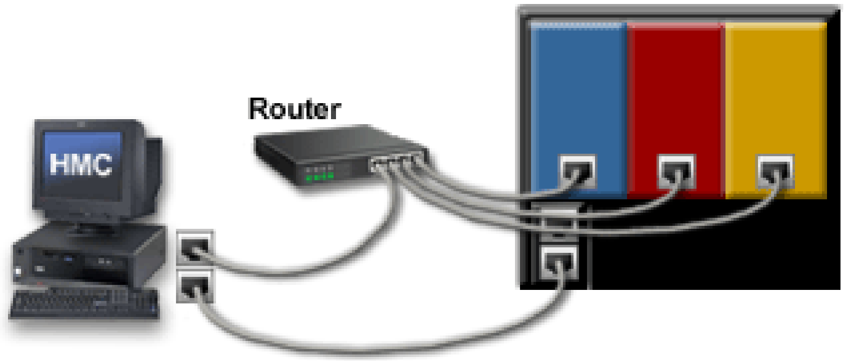
  – Have an Ethernet adapter for one logical partition, most likely your service partition, and then use virtual Ethernet to enable the logical partitions to communicate with each other and with the HMC. This option is the preferred option because it requires that you have only one physical adapter in the system. The following illustration shows this configuration:



  For more information about logical partition communications and virtual Ethernet, see Communication options for logical partitions.

  If you plan to connect this private network to your company network or to an open network, such as the Internet, see Private and open networks in the HMC environment for more information.

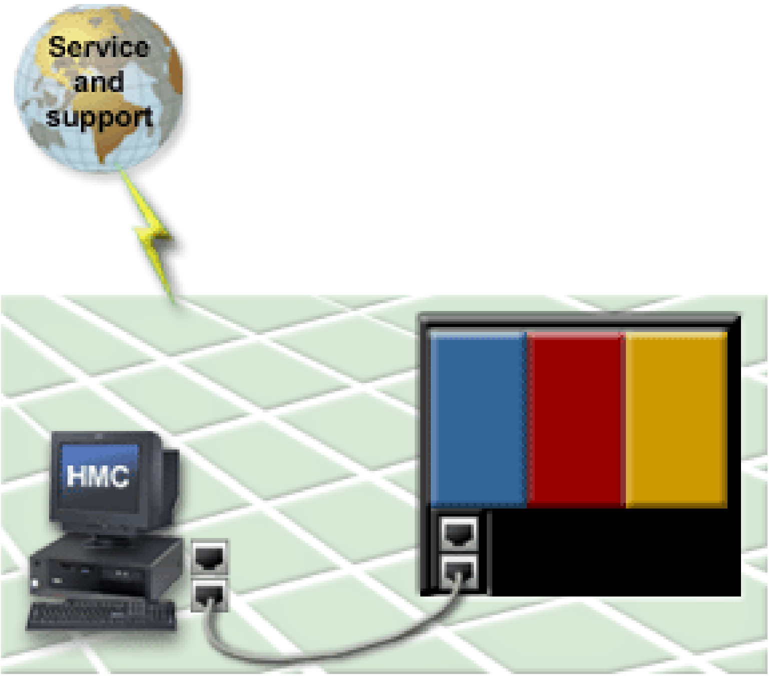
  – Have a LAN adapter for each logical partition, then have a physical connection between each logical partition and the HMC. This option requires that you have a router and a physical LAN adapter for each logical partition. The following illustration shows this configuration:



If you plan to connect this private network to your company network or to an open network, such as the Internet, see Private and open networks in the HMC environment for more information.

- Connection between your company and your service provider

  This connection is the one that enables you to report hardware problems and other server information to your service provider. It also enables you to install fixes. This connection is represented in the following illustration:



This connection will be different depending on how your server is configured and the operating systems you have installed. In some cases, the connection might be through your HMC; in other cases, you might connect directly to your service provider from your server. To understand what these configurations and connections can be, and to decide which connection you might use, see Scenarios: Service and support. For specific information about how to set up your service environment, see Setting up your service environment.

## Setting up your HMC to connect to your service provider

If you have a Hardware Management Console, you must first set up your HMC, including the service environment, before you can set up your server. This section provides an overview of the tasks that are required to set up the HMC for service.

**Choosing your connection method**
This topic describes the different methods you can use to share problem information and system information with your service provider and explains the criteria you should use to make your selection.

**Specifying your company's contact and account information**
This topic describes how to specify the contact and account information on the HMC.

**Specifying options for connection monitoring**
This topic describes how to specify options on the HMC for connection monitoring.

**Configuring Electronic Service Agent on your HMC**
This topic describes how to configure Electronic Service Agent on your HMC.

**Choosing your connection method:** One of your first tasks is to specify how you want the electronic connection to your service provider to be set up. This connection can be through your Hardware Management Console or, in some cases, through a pass-through system, such as another HMC or a logical partition on your server. When deciding which type of connection to use, consider the following:

- **Fix strategy—** The connection type that you select here also dictates how you will install your fixes. For example, if you choose to connect to your service provider through your HMC, you will install server firmware fixes through your HMC.

  For AIX and Linux logical partitions, you will also receive operating system fixes through the HMC. You will then have to make those fixes available to the logical partition or partitions that are running that operating system.

  For i5/OS logical partitions, you use the normal i5/OS PTF installation functions on your service partition for installing fixes rather than using the HMC. For more information on i5/OS fixes, see Maintain and manage i5/OS and related software.
- **Speed —** Different connection types offer different rates of data transfer. Try to select the fastest method of sending and receiving data that you have available to you. For example, a high-speed Internet connection is faster than a modem connection.
- **Location—** The location of the connection is another important factor in your decision. A local connection is preferred to a remote connection; however, you should consider speed and locale together when you make your selection.

The recommended order of connection types by locale and speed is as follows:

1. Local high-speed connection
2. Remote high-speed connection
3. Local modem
4. Remote modem

Use the Remote Support application on the HMC to specify which kind of connection you want to use. To specify this information, follow these steps on your HMC:

1. In the navigation area, open Service Applications.
2. Select **Remote Support**.
3. Select **Customize Outbound Connectivity**.

The options you can specify on the HMC are as follows:

- **Local Modem**

  This option enables you to send problem information and system data to your service provider using the modem on your HMC. You may want to select this option if the following are true:
  - Your HMC does not have a high-speed Internet connection.
  - You do not have any i5/OS logical partitions with high-speed Internet connections.

For more information about how you can use this connection type in your environment, see the following scenarios:

  - Scenario: Multiple AIX logical partitions with an HMC
  - Scenario: Multiple i5/OS logical partitions using the HMC modem

- **Internet VPN**

  This option enables you to send problem information to your service provider using a high-speed Internet connection on your HMC. This is the fastest option available on the HMC, but some companies restrict this type of connection for security reasons. Before you select this option, be sure your company's security policy permits this type of connection.

- **Connecting through other systems or logical partitions**

  This option enables you to send problem information to your service provider through a pass-through system. This pass-through system can be another HMC or a logical partition on your server that supports the Layer 2 Tunneling Protocol (L2TP). Currently, only logical partitions with the V5R3 level of i5/OS can support L2TP and so are the only logical partitions that can be used as pass-through systems.

  You may want to select this option if the following are true:

  - Your HMC does not have a high-speed Internet connection.
  - You have an i5/OS logical partition running V5R3.

  For more information about how you can use this connection type in your environment, see Scenario: Multiple i5/OS logical partitions using VPN on an i5/OS logical partition.

**Specifying your company's contact and account information:** It is important that you specify contact and account information. This information helps your service provider contact the correct person in your company in the event of a system problem. It also helps your service provider locate any information about your company's service history, which may help solve a problem more quickly.

Use the Remote Support application on the HMC to specify your contact and account information. To specify this information, follow these steps on your HMC:

1. In the navigation area, open Service Applications.
2. Select **Remote Support**.
3. Select **Customize Customer Information**.

**Specifying options for connection monitoring:** Connection monitoring enables the monitoring of the communication paths between your HMC and your managed systems and create service events when communication between the HMC and a managed system is disrupted. You can specify the following information about how you want the HMC to respond to these disruptions:

- **Number of disconnected minutes considered an outage:** This is the number of minutes that you want your HMC to wait before reporting a disruption in communication as an outage. The recommended length of time is 15 minutes.
- **Number of connected minutes considered a recovery:** This is the number of minutes after communication is restored between the HMC and the managed system that you want the HMC to wait before considering that a recovery is successful. The recommended length of time is 2 minutes.
- **Number of minutes between outages considered a new incident:** This is the number of minutes after communication is restored that you want the HMC to wait before considering another outage as a new incident. The recommended length of time is 20 minutes.

To specify your preferences for connection monitoring, use the Service Focal Point application on the HMC. To specify this information, follow these steps on your HMC:

1. In the navigation area, open Service Applications.
2. Select **Service Focal Point**.
3. Select **Service Utilities**.

4. On the Service Utilities window, select **Connection Monitoring** from the Actions menu.

After you specify these settings, you can use the **Notification** tab to enable Service Focal Point to send information about the communication problems to Electronic Service Agent. You can then configure Electronic Service Agent to notify you of these problems. For more information, see Configuring Electronic Service Agent on your HMC.

**Configuring Electronic Service Agent on your HMC:** You can use Electronic Service Agent on your HMC to share server information and hardware problem information with your service provider and to receive notification when problems occur. In addition, you can authorize individuals in your organization to view the information you send on the Internet. This enables you to view your history and track any trends in the service information that you share.

The types of server information you can share with your service provider include the following:

- Hardware problem information
- Information about system characteristics, such as hardware and software inventory, and current fix levels
- Information about system resources, such as Capacity on Demand data and disk use
- Performance data

For more information about setting up Electronic Service Agent on your HMC, see the following:

**Specifying when and how Electronic Service Agent sends information to your service provider**
This topic describes how to specify the time of day when your system information is sent and the frequency with which it is sent.

**Setting up notifications for service events**
This topic describes how you can be notified when hardware problems occur on your server.

**Viewing your system information on the Internet**
This topic describes how to set up an account so that you can view your information on the Internet.

*Specifying when and how Electronic Service Agent sends information to your service provider:* Use Electronic Service Agent to define the timetable on which you want to share service information with your service provider and to designate whether you want to optionally send your service information to your service provider using File Transfer Protocol (FTP).

To specify the information to define the timetable, follow these steps:

1. In the navigation area, open **Service Applications**.
2. Select **Service Agent**.
3. Select **Transmit Service Information**.
4. In the Transmit Service Information window, click the **Transmit** tab.
5. To send your information to your service provider immediately, click **Send**.
6. To schedule when and how often you send information to your service provider, select **Schedule when to transmit the service information**, and specify the frequency and time.

You can optionally use File Transfer Protocol (FTP) to send your service information to your service provider. FTP is an alternative way to offload large data files associated with problems that occur on your system.

To specify the information to send service information using FTP, follow these steps:

1. In the navigation area, open **Service Applications**.

2. Select **Service Agent**.
3. Select **Transmit Service Information**.
4. In the Transmit Service Information window, click the **FTP** tab.
5. Select **Enable FTP offload of service information**.
6. Specify the information about the FTP server to which you want to send the service information.
7. If your network includes a firewall, select **Enable firewall configuration settings**, and specify the information about the firewall to enable you to use FTP to offload service information.

*Setting up notifications for service events:* Electronic Service Agent enables you or designated servers to receive notification when service events occur. For example, you can specify e-mail addresses that can be used to notify you or others when problems occur on the server. In addition, you can configure SNMP trap support on the HMC to notify designated servers when problems occur. See the following information for details:

**E-mail notification**

Use Electronic Service Agent to specify e-mail addresses that can be used to notify you or others in your company if there are problems on your server. You can choose whether these e-mail addresses are notified of all problem events or just those that are called in automatically to your service provider. If you have a mobile telephone that supports e-mail, you could use that account to receive notifications while traveling. To specify the e-mail addresses you want to notify, follow these steps:

1. In the navigation area, open **Service Applications**.
2. Select **Service Agent**.
3. Select **Customer Notification**.
4. In the Notification of Service Events window, click the **Email** tab.
5. Select **Enable email notification for problem events**.
6. In the **SMTP server** field, type the IP address or host name of the mail server, and click **Add** to add an e-mail address to the list.

**Simple Network Management Protocol (SNMP) trap support notification**

**Note:** SNMP trap support notification requires that you use Simple Network Management Protocol (SNMP) to allow communication between SNMP managers and SNMP agents using TCP/IP for a transport layer.

For more information on SNMP, see the following Request for Comments (RFCs):

- RFC1155 — Structure and Identification of Management Information for TCP/IP-based Internets
- RFC1157 — A Simple Network Management Protocol (SNMP)
- RFC1213 — Management Information Base for Network Management of TCP/IP based internets: MIB-II
- RFC1592 — Simple Network Management Protocol, Distributed Protocol Interface Version 2

To view the RFCs, see RFC Editor .

Use Electronic Service Agent to specify IP addresses or host names of servers you want to receive notification (SNMP trap) when problems occur. When the server receives notification that a service event has occurred, you can use a program application to process or display the information contained in the notification.

For information about the contents of the traps, see SNMP traps.

To specify the IP addresses or host names of the servers you want to notify, follow these steps:

1. In the navigation area, open **Service Applications**.
2. Select **Service Agent**.
3. Select **Customer Notification**.
4. In the Notification of Service Events window, click the **SNMP Traps** tab.
5. Select **Enable SNMP traps notification**.
6. Click **Add** to add an IP address or host name of the server to the list and to select the notification event.

*SNMP traps:* If you configure Electronic Service Agent to notify servers of service events using SNMP traps, you might want to create programs that display or parse the information contained in the trap. To do that, you need to know what kind of trap is being sent and the contents of the trap.

Use the following information to learn about the kind of traps that Electronic Service Agent might send to your server.

| Generic Trap | Specific Trap | Variable List | Description |
|---|---|---|---|
| enterprise specific (6) | 3 | cpsSystemSendTrap | Problem Log Entry Created<br>Generated when a problem is added to a problem log on a converged power system.<br>`cpsSystemNotifyTrap='yyyy/MM/dd hh:mm:ss tzn\n`<br>` Manufacturer=IBM\n`<br>` ReportingMTMS=tttt-mmm*ppzzzzz\n`<br>` ProbNm=nnnnn\n`<br>`LparName=lparname\n`<br>` FailingEnclosureMTMS=tttt-mmm*ppzzzzz\n`<br>` SRC=ssssssssss\n`<br>` EventText=79 char string\n`<br>` Fru1Info=71 char string\n`<br>` Fru2Info=71 char string\n`<br>` Fru3Info=71 char string\n`<br>Where:<br>**\n** = RETURN<br>**yyyy** = year<br>**MM** = month<br>**dd** = day<br>**hh** = hour(24)<br>**mm** = minute<br>**ss** = seconds<br>**tzn** = time zone<br>**tttt** = type number (for example, 2107)<br>**mmm** = model number (for example, 921)<br>**pp** = plant of manufacture (for example, 75)<br>**zzzzz** = sequence number (for example, FA123)<br>**nnnnn** = problem number<br>**lparname** = logical partition name<br>**ssssssssss** = system reference code<br>**FruNInfo** = information about FRU N, where n is 1,2,3 |

*Viewing your system information on the Internet:* The information you share through Electronic Service Agent is available for you to view on the Internet. You can view your current information, as well as track trends in performance and usage. This online service is available to you while your server is under warranty and afterward through a service contract.

Before you can access your information on the Internet, you must complete a registration process. For security reasons, this registration process involves the following steps:

1. Register users with IBM on the My IBM Registration Web site.

   On the registration Web site, you create an IBM ID for each of the people you want to have access to the information that Electronic Service Agent shares with IBM. You must associate these accounts with a server, usually your central server. (You can add other servers later if you want to share information for other servers on your network.) The people for whom you create IDs must have system administrator authority on all registered servers.

2. Submit a registration request from Electronic Service Agent, as follows:
   a. In the navigation area, open Service Applications.
   b. Select **Service Agent**.
   c. Select **Service Registration**. The Authorize Users for Service Agent window is displayed.
   d. In the Web authorization section, specify one or two of the user IDs that you created on the IBM Registration Web site.
   e. Click **OK** to submit the registration request. You can specify only two IBM IDs at one time, but you can submit as many registration requests as you like.

When you want to view the server information you have shared with IBM, go to IBM Electronic Services.

## Setting up your server to connect to your service provider

After you have configured your HMC, you must set up the connection to your service provider. This connection can provide two-way communication between your server and your service provider. Each operating environment has requirements to consider when you set up your connections. The following links help you understand the requirements for your operating environment.

**Setting up AIX to connect to your service provider**
This topic describes how to set up your AIX logical partition to connect to your service provider.

**Setting up i5/OS to connect to your service provider**
This topic describes how to set up your i5/OS logical partition to connect to your service provider.

**Setting up Linux to connect to your service provider**
This topic describes how to set up your Linux logical partition to connect to your service provider.

**Setting up the service processor to connect to your service provider**
This topic describes how to set up your service processor to connect to your service provider.

**Setting up AIX to connect to your service provider:** If you are running AIX on your server, you can create a connection from your server to the service provider through either the modem or a direct Internet connection. The following example demonstrates how to create the service connection through the modem.

To connect to your service provider through the modem on your server, you need to configure Electronic Service Agent on your servers or logical partitions running AIX. Read the following information to become familiar with basic terminology and the steps you need to perform to configure Electronic Service Agent on your server. For complete configuration instructions, go to the Electronic Service Agent Web site and search for the appropriate Electronic Service Agent user's guide.

**Terminology**

You need to be familiar with the following terms before you configure Electronic Service Agent on the servers or logical partitions:

- **Service Agent Connection Manager**
  The application that enables the gateway server and client servers to use a single, secure connection to reach the service provider. The connection to the service provider might be using a modem or a direct Internet connection.

- **Service Agent gateway**
  Server or logical partition that acts as the central management server for all of the clients (monitored servers or logical partitions). The SA gateway server contains the central database, and it initiates communication to the service provider.
- **Service Agent clients**
  The monitored machines or logical partitions for which system information is collected and reported to the service provider.

**Configuration steps**

To configure Electronic Service Agent, you need to perform a number of steps from the following AIX interfaces:

- System Management Interface Tool (SMIT)
- Service Agent Basic User Interface

You need to complete the following steps to configure Electronic Service Agent. Use these steps as a guide to understand what you need to do to set up your service connection. However, for complete configuration instructions, go to the Electronic Service Agent Web site and search for the appropriate Electronic Service Agent user's guide.

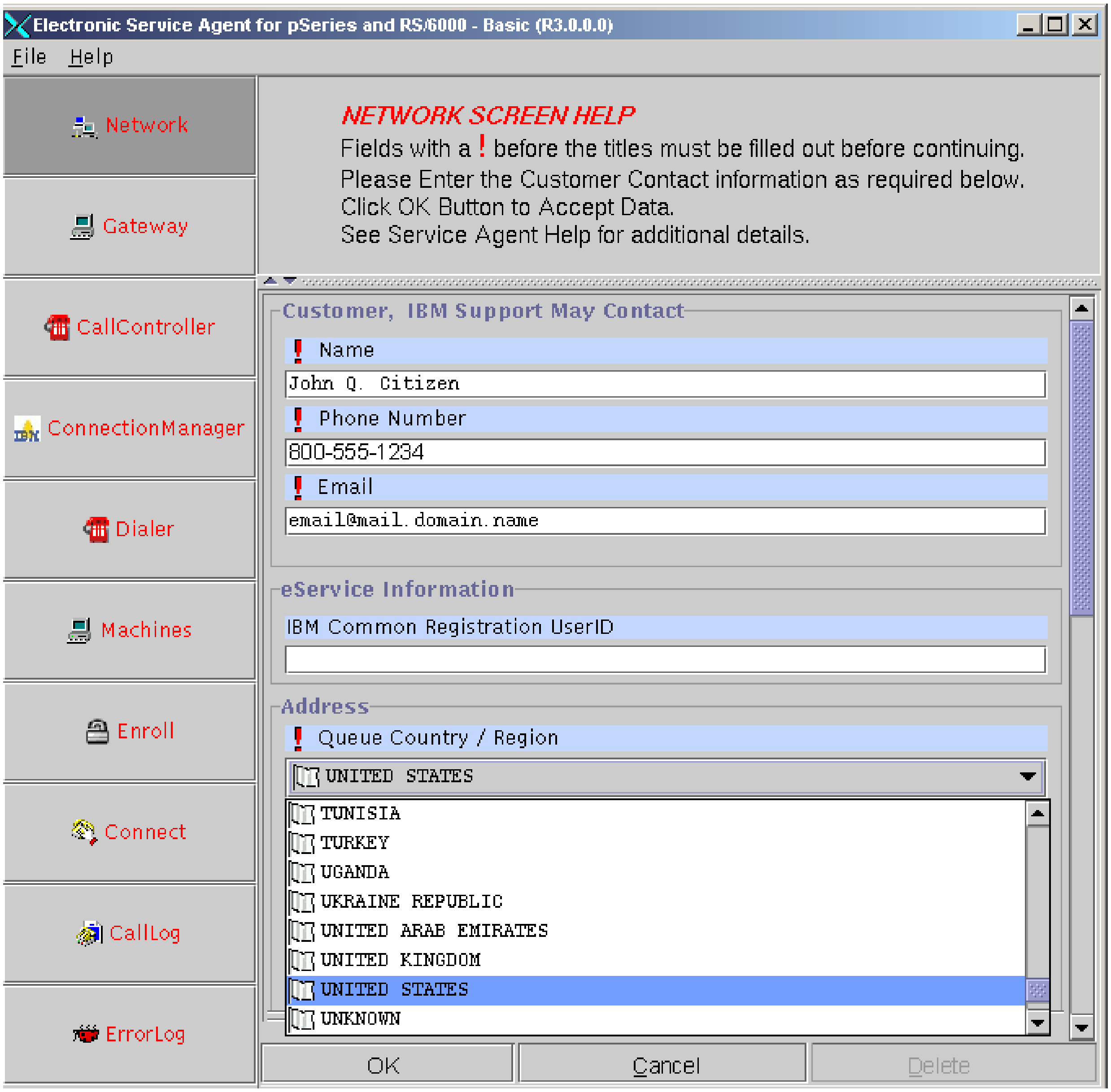
**From the System Management Interface Tool (SMIT), follow these steps:**

1. Configure and start Service Agent Connection Manager (SACM).
   - Verify that the host name for the SACM is correct. In this example, the SACM resides on the server or logical partition with the modem. Therefore, the SACM is configured to the host name of the server or logical partition with the modem.
   - Verify the default port 1198. In most cases, the default port is appropriate. You can change the port later, if necessary.
2. Configure and start the Service Agent gateway server.
   - Verify that the host name is correct. In this example, the SA gateway server is the server or logical partition with the modem. Therefore, the SA gateway is configured to the host name of the server or logical partition with the modem.
   - Verify that the machine type, model and serial number are correct.
3. Configure and start the Service Agent client servers.
   - Verify that the host names for the SA client servers and for the SA gateway are correct.
   - Verify that the machine type, model and serial number are correct.

**From the Service Agent Basic User Interface, follow these steps:**

1. Get familiar with the Service Agent Basic User Interface
   The SA Basic User Interface provides a list of properties and the associated fields that you need to

complete to configure Electronic Service Agent, as shown in the figure below.



NETWORK SCREEN HELP

Fields with a ! before the titles must be filled out before continuing.
Please Enter the Customer Contact information as required below.
Click OK Button to Accept Data.
See Service Agent Help for additional details.

Customer, IBM Support May Contact

! Name: John Q. Citizen

! Phone Number: 800-555-1234

! Email: email@mail.domain.name

eService Information

IBM Common Registration UserID:

Address

! Queue Country / Region: UNITED STATES

2. Specify information for the required property fields

   Click each property on the left side of the interface, and complete the required fields on the right side of the interface. Required fields are indicated with an exclamation point.

   Depending on how you complete the fields, the interface automatically guides you through the appropriate properties. For example, if you specify that you want to use a modem in the ConnectionManager property fields, the interface automatically displays the Dialer property fields, so that you can complete the information about your modem.

   For this example, where you have multiple servers or logical partitions running AIX and you use a modem for outbound connectivity, you need to complete specific information for the following properties:

   - **ConnectionManager** — Uncheck **False** for **Connect to SDR using Dialer** to enable the Dialer. This indicates that you want to use a modem to connect to your service provider.
   - **Dialer** — Specify details about your modem and your service provider connection parameters.
   - **Machines** — Add two SA client servers.

- **Enroll —** Register the servers with the service provider. This initiates a call to the service provider to enroll the servers in the service provider's database. To complete the process, the service provider sends you a key.
- **Call log —** Check the status of the call to the service provider. You can see whether the call to the service provider is successful.

You have completed the steps for the basic Electronic Service Agent configuration for this example. To learn about advanced features that go beyond the scope of this example, go to the Electronic Service Agent Web site and search for the appropriate Electronic Service Agent user's guide.

**Setting up i5/OS logical partitions to connect to your service provider:** You can use any of the following methods to create the service connection from your i5/OS logical partitions to your service provider.

**Setting up i5/OS to connect to your service provider using VPN**
Learn how to create a service connection to send service information from i5/OS to your service provider using a VPN connection from the i5/OS logical partition.

**Setting up i5/OS to connect to your service provider using the modem on server**
Learn how to create a service connection to send service information from i5/OS to your service provider using the modem on the i5/OS logical partition.

**Setting up i5/OS to connect to your service provider through the HMC**
Learn how to create a service connection to send service information from i5/OS to your service provider using the modem on the HMC.

*Setting up i5/OS to connect to your service provider using VPN:* You can use one of several methods to connect to your service provider through a VPN connection on an i5/OS logical partition. Each method provides a way to create the connection between your i5/OS logical partition and your service provider, and each method offers certain advantages.

Read the following information to learn about each method:
- Simplified activation
- Universal Connection wizard
- Extreme Support wizard

Optionally, you can start IBM Performance Management for eServer™ iSeries (PM eServer iSeries or PM iSeries) to maximize your server's application and hardware performance (by using performance trend analysis). PM iSeries uses Collection Services to gather nonproprietary performance and capacity data from your server and send the data to your service provider for analysis. Your service provider stores and protects the data for you and provides you with reports and graphs that show your server's growth and performance.

*Simplified activation:* You can create the connection profiles for electronic customer support and for Electronic Service Agent using the simplified activation method. You use the character-based interface on a 5250 emulator to implement this method.

Simplified activation provides the following advantages:
- Saves you time
  This method can save you time because you can enter contact information, such as company name and address, using the Remote Support Facility (RSF) interface on the HMC. RSF stores the information in the service processor. When you run the simplified activation of Electronic Service Agent, the program retrieves the contact information from the service processor so you do not have to enter it again.
- Sends service information to your service provider
  This method enables your system to automatically send service information to your service provider in

addition to hardware failures. Your service provider can use the service information to proactively provide you with service and support that uniquely fits your needs. When a problem occurs, service personnel can act quickly because they already have the service information needed to analyze and solve the problem.

To implement simplified activation, you need to perform a number of steps from the character-based interface. One of the steps requires you to enter the Create Service Configuration (CRTSRVCFG) command. If you choose to use the simplified activation method to connect to your service provider through a VPN connection on an i5/OS logical partition, specify the following information for the CRTSRVCFG command parameters:

- Connection type: *VPN
- Virtual private network type: *DIRECT
- Connectivity for others:
  - Connection point: *YES

    This enables other logical partitions or systems to use the VPN connection on this logical partition to connect to the service provider.
  - Interfaces: *ALL or a list of the interfaces over which you will accept connections to the service provider.

**Note:** For complete configuration instructions, go to Online Publications and search for the appropriate simplified activation user's guide.

*Universal Connection wizard:* You can use the Universal Connection wizard in iSeries Navigator to create the connection profiles for electronic customer support and for Electronic Service Agent. In addition, you can use this method to download documentation from the iSeries Information Center.

If you choose to use the Universal Connection wizard to connect to your service provider through a VPN connection on an i5/OS logical partition, consider your network configuration to determine which Universal Connection scenario to review:

- If all of your logical partitions have access to the Internet (either each logical partition has its own Ethernet adapter for individual Internet connections or the logical partitions are connected using virtual Ethernet where one logical partition performs proxy ARP and provides a connection to the Internet), refer to Configure a direct Internet connection scenario in the Universal Connection topic. If each logical partition has its own adapter, perform these steps from each logical partition. If the logical partitions are connected using virtual Ethernet, perform these steps from the logical partition that performs proxy ARP.
- If only one of your logical partitions has a connection to the Internet and the other logical partitions are on separate, private networks for security reasons (not directly connected to the Internet), refer to the Configure direct Internet connection from a server that provides connectivity for other systems or logical partitions scenario in the Universal Connection topic; perform these steps from the logical partition that has direct connection to the Internet. Then refer to the Configure a multihop connection through a remote server scenario in the Universal Connection topic; perform these steps from each of the other logical partitions.

*Extreme Support wizard:* You can use the Extreme Support wizard in iSeries Navigator to establish your service connection. If you did not previously configure the connection profiles for electronic customer support or for Electronic Service Agent, you are given the opportunity to configure the connection profiles with the Extreme Support wizard.

The Extreme Support wizard provides the following advantages:

- Sends service information to your service provider

  This method enables your system to automatically send service information to your service provider in addition to hardware failures. Your service provider can use the service information to proactively provide you with service and support that uniquely fits your needs. When a problem occurs, service personnel can act quickly because they already have the service information needed to analyze and solve the problem.

- Consolidates service information from a group of systems
  This method enables you to configure Electronic Service Agent to consolidate the service information from a group of systems before the service information is sent from a central system to your service provider.

If you choose to use the Extreme Support wizard to connect to your service provider through a VPN connection on an i5/OS logical partition, consider your network configuration to determine which Universal Connection scenario to review:

- If all of your logical partitions have access to the Internet (either each logical partition has its own Ethernet adapter for individual Internet connections or the logical partitions are connected using virtual Ethernet where one logical partition performs proxy ARP and provides routability to the Internet), refer to the Configure a direct Internet connection scenario in the Universal Connection topic. If each logical partition has its own adapter, perform these steps from each logical partition. If the logical partitions are connected using virtual Ethernet, perform these steps from the logical partition that performs proxy ARP.
- If only one of your logical partitions has routability to the Internet and the other logical partitions are on separate, private networks for security reasons (not directly routable to the Internet), refer to the Configure direct Internet connection from a server that provides connectivity for other systems or logical partitions scenario in the Universal Connection topic; perform these steps from the logical partition that has direct routability to the Internet. Then, refer to the Configure a multihop connection through a remote server scenario in the Universal Connection topic; perform these steps from each of the other logical partitions.

*Setting up i5/OS to connect to your service provider using the modem on the server:* You can use one of several methods to connect to your service provider through the modem on the server. Each method provides a way to create the connection between your i5/OS logical partition and your service provider, and each method offers certain advantages.

Read the following information to learn about each method:

- Simplified activation
- Universal Connection wizard
- Extreme Support wizard

Optionally, you can start IBM Performance Management for eServer iSeries (PM eServer iSeries or PM iSeries) to maximize your server's application and hardware performance (by using performance trend analysis). PM iSeries uses Collection Services to gather nonproprietary performance and capacity data from your server and send the data to your service provider for analysis. Your service provider stores and protects the data for you and provides you with reports and graphs that show your server's growth and performance.

*Simplified activation:* You can create the connection profiles for electronic customer support and for Electronic Service Agent using the simplified activation method. You use the character-based interface on a 5250 emulator to implement this method.

Simplified activation provides the following advantages:

- Saves you time
  This method can save you time because you can enter contact information, such as company name and address, using the Remote Support Facility (RSF) interface on the HMC. Then, RSF stores the information in the service processor. When you run the simplified activation of the Electronic Service Agent, the program retrieves the contact information from the service processor, so you do not have to enter it again.

- Sends service information to your service provider
  This method enables your system to automatically send service information to your service provider in addition to hardware failures. Your service provider can use the service information to proactively provide you with service and support that uniquely fits your needs. When a problem occurs, service personnel can act quickly because they already have the service information needed to analyze and solve the problem.

To implement simplified activation, you need to perform a number of steps from the character-based interface. One of the steps requires you to enter the Create Service Configuration (CRTSRVCFG) command. If you choose to use the simplified activation method to connect to your service provider through the modem on the server, specify the following information for the CRTSRVCFG command parameters:

Specify the following information from the logical partition that has the modem:

- Connection type: *PTP
- Point to point type: *LOCAL
- Service: *SRVAGT

  Two service configurations will be created. The first one will be used by electronic customer support (ECS) which Electronic Service Agent uses for reporting hardware problems. The second will be used for sending the service information.
- Connectivity for others:
  - Connection point: *YES

    This enables other logical partitions or systems to use the modem on this logical partition to connect to your service provider.
  - Interfaces: *ALL or a list of the interfaces over which you will accept connections to your service provider.

Specify the following information from each of the other i5/OS logical partitions:

- Connection type: *PTP
- Point to point type: *REMOTE
- Service: *SRVAGT

  Two service configurations will be created. The first one will be used by electronic customer support (ECS) which Electronic Service Agent uses for reporting hardware problems. The second will be used for sending the service information.
- Remote system: Enter the IP address for the logical partition through which you will connect to your service provider.

**Note:** For complete configuration instructions, go to Online Publications and search for the appropriate simplified activation user's guide.

*Universal Connection wizard:* You can use the Universal Connection wizard in iSeries Navigator to create the connection profiles for electronic customer support and for Electronic Service Agent. In addition, you can use this method to download documentation from the iSeries Information Center.

If you choose to use the Universal Connection wizard to connect to your service provider through the modem on the server, refer to the Configure a PPP dial-up connection for a server that provides connectivity for other systems through AGNS scenario in the Universal Connection topic; perform these steps on the logical partition that has the modem. Then refer to the Configure a remote PPP dial-up connection scenario in the Universal Connection topic; perform these steps on each of the other logical partitions.

*Extreme Support wizard:* You can use the Extreme Support wizard in iSeries Navigator to establish your service connection. If you did not previously configure the connection profiles for electronic customer support or for Electronic Service Agent, you are given the opportunity to configure the connection profiles with the Extreme Support wizard.

The Extreme Support wizard provides the following advantages:

- Sends service information to your service provider
  This method enables your system to automatically send service information to your service provider in addition to hardware failures. Your service provider can use the service information to proactively provide you with service and support that uniquely fits your needs. When a problem occurs, service personnel can act quickly because they already have the service information needed to analyze and solve the problem.
- Consolidates service information from a group of systems
  This method enables you to configure Electronic Service Agent to consolidate the service information from a group of systems before the service information is sent from a central system to your service provider.

If you choose to use the Extreme Support wizard to connect to your service provider through the modem on the server, refer to the Configure a PPP dial-up connection for a server that provides connectivity for other systems through AGNS scenario in the Universal Connection topic; perform these steps on the logical partition that has the modem. Then refer to the Configure a remote PPP dial-up connection scenario in the Universal Connection topic; perform these steps on each of the other logical partitions.

*Setting up i5/OS to connect to your service provider through the HMC:* You can use one of several methods to connect to your service provider through the modem on the HMC. Each method provides a way to create the connection between your i5/OS logical partition and your service provider, and each method offers certain advantages.

Read the following information to learn about each method:

- Simplified activation
- Universal Connection wizard
- Extreme Support wizard

Optionally, you can start IBM Performance Management for eServer iSeries (PM eServer iSeries or PM iSeries) to maximize your server's application and hardware performance (by using performance trend analysis). PM iSeries uses Collection Services to gather nonproprietary performance and capacity data from your server and send the data to your service provider for analysis. Your service provider stores and protects the data for you and provides you with reports and graphs that show your server's growth and performance.

*Simplified activation:* You can create the connection profiles for electronic customer support and for Electronic Service Agent using the simplified activation method. You use the character-based interface on a 5250 emulator to implement this method.

Simplified activation provides the following advantages:

- Saves you time
  This method can save you time because you can enter contact information, such as company name and address, using the Remote Support Facility (RSF) interface on the HMC. RSF stores the information in the service processor. When you run the simplified activation of the Electronic Service Agent, the program retrieves the contact information from the service processor so you do not have to enter it again.
- Sends service information to your service provider
  This method enables your system to automatically send service information to your service provider in addition to hardware failures. Your service provider uses the service information to proactively provide

you with service and support that uniquely fits your needs. When a problem occurs, service personnel can act quickly because they already have the service information needed to analyze and solve the problem.

To implement simplified activation, you need to perform a number of steps from the character-based interface. One of the steps requires you to enter the Create Service Configuration (CRTSRVCFG) command. If you choose to use the simplified activation method to connect to your service provider through the modem on the HMC, specify the following information for the CRTSRVCFG command parameters:

- Connection type: *PTP
- Point to point type: *REMOTE
- Service: *SRVAGT

  Two service configurations will be created. The first one will be used by electronic customer support (ECS) which Electronic Service Agent uses for reporting hardware problems. The second will be used for sending service information.
- Remote system: Enter the IP address or host name of the interface on the HMC through which you will connect to your service provider.

  **Note:** The HMC might have multiple interfaces with associated IP addresses and host names. For the Remote system parameter, you must specify the interface on the HMC that provides partition communication.

  To find the interface that provides partition communication, follow these steps from 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. Expand **HMC Management**.
  3. Click **HMC Configuration**.
  4. In the contents pane, click **Customize network settings**.
  5. Click the **LAN Adapters** tab.
  6. Select a LAN adapter and click **Details**.
  7. Click the **Lan Adapter** tab.
  8. In the Local Area Network Information section, the Partition communication checkbox indicates whether this interface is used for partition communication.

**Note:** For complete configuration instructions, go to Online Publications and search for the appropriate simplified activation user's guide.

*Universal Connection wizard:* You can use the Universal Connection wizard in iSeries Navigator to create the connection profiles for electronic customer support and for Electronic Service Agent. In addition, you can use this method to download documentation from the iSeries Information Center.

If you choose to use the Universal Connection wizard to connect to your service provider through the modem on the HMC, refer to the Configure a remote PPP dial-up connection scenario in the Universal Connection topic.

*Extreme Support wizard:* You can use the Extreme Support wizard in iSeries Navigator to establish your service connection. If you did not previously configure the connection profiles for electronic customer support or for Electronic Service Agent, you are given the opportunity to configure the connection profiles with the Extreme Support wizard.

The Extreme Support wizard provides the following advantages:

- Sends service information to your service provider
  This method enables your system to automatically send service information to your service provider in addition to hardware failures. Service personnel can use the service information to proactively provide you with service and support that uniquely fits your needs. When a problem occurs, service personnel can act quickly because they already have the service information needed to analyze and solve the problem.
- Consolidates service information from a group of systems
  This method enables you to configure Electronic Service Agent to consolidate the service information from a group of systems before the service information is sent from a central system to your service provider.

If you choose to use the Extreme Support wizard to connect to your service provider through the modem on the HMC, refer to the Configure a remote PPP dial-up connection scenario in the Universal Connection topic for configuration details.

**Setting up Linux to connect to your service provider:** If you are running Linux on your server, you can create a connection from your server to the service provider through either a modem or a direct Internet connection. The following example demonstrates how to create the service connection through the modem.

To connect to your service provider through the modem on your server, you need to configure Electronic Service Agent on your servers running Linux. Read the following information to become familiar with basic terminology and the steps you need to perform to configure Electronic Service Agent on your server. For complete configuration instructions, go to the Electronic Service Agent Web site and search for the appropriate Electronic Service Agent user's guide.

**Terminology**

You need to be familiar with the following terms before you configure Electronic Service Agent on the servers:

- **Service Agent Connection Manager**
  The application that enables the gateway server and client servers to use a single, secure connection to reach the service provider. The connection to the service provider might be using a modem or a direct Internet connection.
- **Service Agent gateway**
  Server that acts as the central management server for all of the clients (monitored servers). The SA gateway server contains the central database, and it initiates communication to the service provider.
- **Service Agent clients**
  The monitored machines for which system information is collected and reported to the service provider.

**Configuration steps**

To configure Electronic Service Agent, you need to perform a number of steps from the following interfaces:

- Linux command line
- Service Agent Basic User Interface

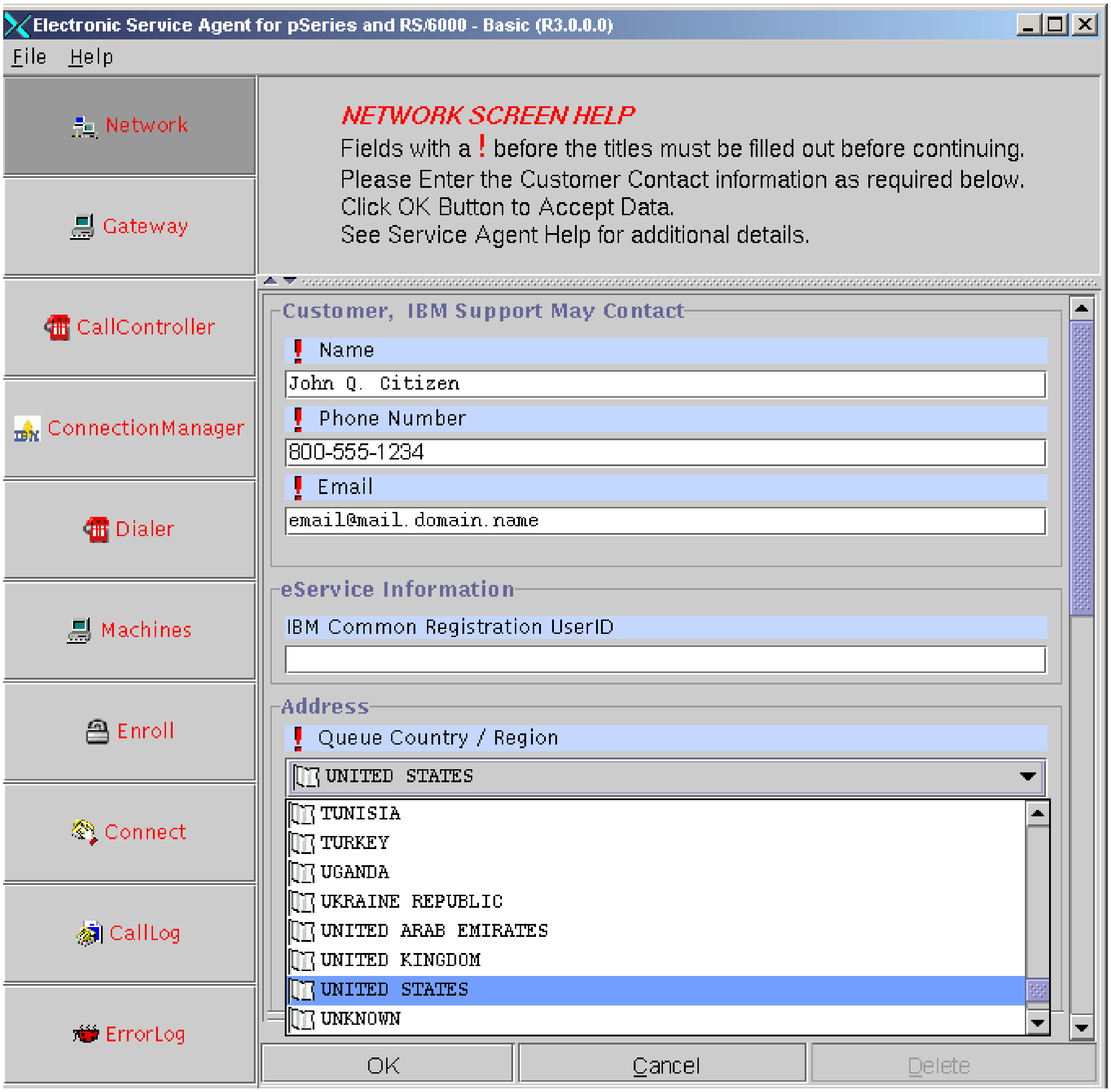
You need to complete the following steps to configure Electronic Service Agent. Use these steps as a guide to understand what you need to do to set up your service connection. However, for complete configuration instructions, go to the Electronic Service Agent Web site and search for the appropriate Electronic Service Agent user's guide.

**From the Linux command line, follow these steps:**

1. Configure and start Service Agent Connection Manager (SACM).
   At a Linux command line, type:
   ```
   startsrc –s sacm
   ```
2. Configure and start the Service Agent gateway server.
   At a Linux command line, type:
   ```
   /usr/svcagent/bin/sagatewayconfig
   ```
3. Configure and start the Service Agent Client servers.
   At a Linux command line, type:
   ```
   startsrc -g svcagent
   ```

**From the Service Agent Basic User Interface, follow these steps:**

1. Get familiar with the Service Agent Basic User Interface
   The SA Basic User Interface provides a list of properties and the associated fields that you need to complete to configure Electronic Service Agent, as shown in the figure below.



*NETWORK SCREEN HELP*
Fields with a ! before the titles must be filled out before continuing.
Please Enter the Customer Contact information as required below.
Click OK Button to Accept Data.
See Service Agent Help for additional details.

Customer, IBM Support May Contact

! Name: John Q. Citizen

! Phone Number: 800-555-1234

! Email: email@mail.domain.name

eService Information

IBM Common Registration UserID:

Address

! Queue Country / Region: UNITED STATES

TUNISIA
TURKEY
UGANDA
UKRAINE REPUBLIC
UNITED ARAB EMIRATES
UNITED KINGDOM
UNITED STATES
UNKNOWN

2. Specify information for the required property fields

Click each property on the left side of the interface, and complete the required fields on the right side of the interface. Required fields are indicated with an exclamation point.

Depending on how you complete the fields, the interface automatically guides you through the appropriate properties. For example, if you specify that you want to use a modem in the ConnectionManager property fields, the interface automatically displays the Dialer property fields, so that you can complete the information about your modem.

For this example, where you have multiple servers running Linux and you use a modem for outbound connectivity, you need to complete specific information for the following properties:

- **ConnectionManager —** Select **True** for **Use modem as a connection method to IBM** to enable the Dialer. This indicates that you want to use a modem to connect to your service provider.
- **Dialer —** Specify details about your modem and your service provider connection parameters.
- **Machines —** Add two SA Client servers.
- **Enroll —** Register the servers with the service provider. This initiates a call to the service provider to enroll the servers in the service provider's database. To complete the process, the service provider sends you a key.
- **Call log —** Check the status of the call to the service provider. You can see whether the call to the service provider is successful.

You have completed the steps for the basic Electronic Service Agent configuration for this example. To learn about advanced features that go beyond the scope of this example, go to the Electronic Service Agent Web site and search for the appropriate Electronic Service Agent user's guide.

**Setting up the service processor to connect to your service provider:** If your server is in its manufacturing default configuration, you can set up your service processor to connect to your service provider. You might use this type of service connection if your server is not available, because the service processor does not require an operating system to perform its tasks.

To set up your service processor to connect to your service provider, you need to attach a modem to the service processor serial port on your server. In addition, you need to use the Advanced System Management Interface (ASMI) menus to perform several configuration steps.

**Note:** If you have i5/OS installed, it is not necessary for you to set up the service processor to call your service provider because this is handled by i5/OS. For more information, see Setting up i5/OS to connect to your service provider.

To set up the service processor to connect to your service provider, follow these steps:

1. Configure a serial port
2. Configure the modem
3. Configure call-home and call-in policy
4. Test the connection

## Testing the connection to your service provider

After you have set up your server to communicate with your service provider, follow the procedures here to test your connection.

**Prerequisites:**

- Your server hardware is installed and functional.
- Your operating system is installed and functional.
- You have performed all the procedures for setting up your HMC (or your server if you do not use an HMC) to call out to your service and support provider.
- Your Electronic Service Agent server's connection to your service provider is set up (for example, the network or modem connections are in place).

From the following list, choose the test instructions that allow you to test the connection for your operating environment:

Testing the connection using your HMC
Learn how to test the connection using the HMC.

Testing the connection using i5/OS
Learn how to test the connection using the character-based interface on the 5250 emulator or using iSeries Navigator for the logical partition that runs i5/OS.

Testing the connection using AIX
Learn how to test the connection for the partition running AIX.

Testing the connection using Linux
Learn how to test the connection for the partition running Linux.

**Testing the connection using your HMC:** If you are using an HMC, use this method of testing your connection to your service provider. To test your connection, do the following:

1. In the navigation area, open Service Applications.
2. Select **Remote Support**.
3. Select **Customize Outbound Connectivity**.
4. Select the tab for the type of outbound connectivity you chose for your HMC (Local Modem, Internet VPN, or Pass-Through Systems). For more information on these settings, see Choosing your connection method.
5. Click **Test**.

**Testing the connection using i5/OS:** You can test the connection to your service provider using either the character-based interface on the 5250 emulator or using iSeries Navigator. To test the connection, you can test either the Electronic Service Agent connection profile or the electronic customer support connection profile.

To learn how to test the service connection, read the following:

To test the Electronic Service Agent connection profile, use either the character-based interface or iSeries Navigator:

- Using the character-based interface, follow these steps:
  1. At the command line, type `GO SERVICE`.
  2. From the Electronic Service Agent menu, select option 3 (Service Information Collection), and press Enter.
  3. From the Service Information Collection menu, select option 6 (Verify Service Connection), and press Enter. A message is displayed that indicates whether the test connection is successful.
- Using iSeries Navigator, follow these steps:
  1. In iSeries Navigator, expand the **Management Central server > Extreme Support > Agents**.
  2. In the right pane, right-click **Electronic Service Agent**, and select **Verify connection to IBM**. A dialog is displayed that indicates whether the test connection is successful.

  **Note:** If you create the Electronic Service Agent connection profile using the Universal Connection wizard, you can verify the connection after you complete the wizard. After you click **Finish** to complete the wizard, a dialog is displayed. To test the connection, click **Test** on the dialog.

To test the electronic customer support connection profile, use either the character-based interface or iSeries Navigator:

- Using the character-based interface, type SNDSRVRQS *TEST at the command line. A message is displayed that indicates whether the test connection is successful.
- Using the Universal Connection wizard in iSeries Navigator, you can create the electronic customer support connection profile, and you can verify the connection. After you click **Finish** to complete the wizard, a dialog is displayed. To test the connection, click **Test** on the dialog.

**Testing the connection using AIX:** To test your AIX connection to your service provider, follow these steps:

1. From the System Management Interface Tool (SMIT) on your Electronic Service Agent server, activate the Electronic Service Agent.
2. Ensure that the Electronic Service Agent Connection Manager is active if it resides on a machine other than the Electronic Service Agent server.
3. From SMIT, start the Service Agent Advanced User Interface.
4. To use a modem, configure the Dialer on the Connection Manager screen.

   **Note:** Default is to connect to the service provider using an existing Internet connection.
5. Open the **Manual Tools** folder.
6. Select **Connect**.
7. Monitor the CallLog for the following entry: TEST Connection (Success: 1, Fail: 0).

**Testing the connection using Linux:** To test your Linux connection to your service provider, follow these steps:

1. On your Electronic Service Agent server, activate the Electronic Service Agent.

   At a Linux command line, type the following:

   ```
   startsrc -g svcagent
   ```
2. Ensure that the Electronic Service Agent Connection Manager is active if it resides on a machine other than the Electronic Service Agent server.

   At a Linux command line, type the following:

   ```
   startsrc -s sacm
   ```
3. Start the Service Agent Advanced User Interface.

   At a Linux command line, type the following:

   ```
   /usr/svcagent/bin/sauiascii
   ```
4. If you want to use a modem, configure the Dialer on the Connection Manager screen.

   **Note:** Default is to connect to the service provider using an existing Internet connection.
5. Open the **Manual Tools** folder.
6. Click **Connection**.
7. Monitor the CallLog for the following entry: TEST Connection (Success: 1, Fail: 0).

## Customizing your service settings

After you have your service environment set up, there are some settings that you may want to change based on your company's needs. The following topics describe how to change some of these service settings:

**Specifying when and how often Electronic Service Agent sends information to your service provider**
Use the information in this topic to change how Electronic Service Agent shares information with your service provider.

**Setting up notifications for service events**
Use the information in this topic to set up or change how you are notified of problems on your system.

**Viewing your system information on the Internet**
Use the information in this topic to modify the list of users who can view your system information on the Internet.

**Specifying options for connection monitoring**
Use the information in this section to change the options you use for watching the communication paths between your HMC and its managed systems.

## Reporting problems

You can set up your server so that hardware problems are reported electronically. For information on how to set up your service environment, see Setting up your service environment. However, if there is a failure in your default service path (for example, the HMC is not available), you can use other ways to ensure that these problems are still reported electronically.

**Reporting problems when the HMC is not available**
Use the information in this topic to understand how you can ensure that problems are reported even if your HMC is not available.

**Reporting problems when your server is down**
Use the information in this topic to understand what you can do to ensure that hardware problems are reported even if your server is down.

### Reporting problems when the HMC is not available

Depending on how you have set up your service environment, your HMC might be reporting hardware errors and sending server information to your service provider. However, if your HMC is not available, you need another way to report these problems. You can designate one of your logical partitions to be the *service partition*, which means that it has the authority to update the server firmware and set other policy parameters without having to power off the server.

The logical partition you choose to act as the service partition depends on your server model and the operating systems running on your partitions. For detailed information, see Service partition.

If your service partition runs i5/OS, the operating system can monitor the communication path between the server and the HMC. If the HMC does not respond, i5/OS has the ability to automatically report hardware problems.

### Reporting problems when the server is down

The service processor is part of your platform hardware and monitors hardware attributes and conditions on your server. The service processor is controlled by server firmware and does not require an operating system to perform its tasks. For this reason, the service processor can report hardware problems on your server, even when the server is not available. This method of reporting problems is only available if your server is in its manufacturing default configuration. If you have i5/OS installed, it is not necessary for you to set up the service processor to call your service provider because this is handled by i5/OS. For more information, see Setting up i5/OS to connect to your service provider.

You use the Advanced System Management Interface (ASMI) to set up problem reporting on the service processor. You can access the ASMI using your HMC, any PC on your network that has a Web browser installed on it, or an ASCII terminal. For more information about how to set up a connection to the Advanced System Management Interface, see Accessing the Advanced System Management Interface. For information on how to set up call-out on your service processor, see Setting up the service processor to connect to your service provider.

For information about the other tasks you can do with the service processor, see Managing your server using ASMI.

## Getting fixes

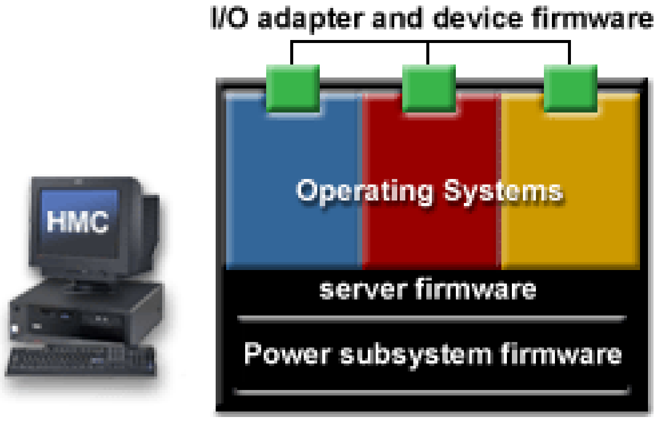
Fixes provide changes to your software, Licensed Internal Code, or machine code that fix known problems, add new function, and keep your server or Hardware Management Console operating efficiently. For example, you might install fixes for your operating system in the form of a PTF (program temporary fix). Or, you might install a server firmware fix (also known as a Licensed Internal Code fix) with code changes that are needed to support new hardware or new functions of the existing hardware.

A good fix strategy is an important part of maintaining and managing your server. You should install fixes on a regular basis if you have a dynamic environment that changes frequently. If you have a stable environment, you do not have to install fixes as frequently. However, you should consider installing fixes whenever you make any major software or hardware changes in your environment.

You can get fixes using a variety of methods, depending on your service environment. For example, if you use an HMC to manage your server, you can use the HMC interface to download, install, and manage your HMC and server firmware fixes. If you do not use an HMC to manage your server, you can use the functions specific to your operating system to get your fixes.

In addition, you can download or order many fixes through the Internet. From Fix Central, you can search by server and product to find the latest fixes for your system's software, hardware, and operating system.

You must manage several types of fixes to properly maintain your hardware. The following figure shows the different types of hardware and software that might require fixes.



Read about each type of fix to learn more about fixes and to determine the best method to get fixes in your environment:

**Note:** If you use an HMC to manage your system and you are setting up the server for the first time or upgrading to a new server firmware release, it is recommended that you install the HMC fixes before you install the server firmware fixes.

**HMC fixes**
Use the information in this section to learn how to download fixes for the machine code on your HMC.

**Server firmware fixes**
Server firmware is the code that enables hardware, such as the service processor. Use the information in this section to download, install, and manage fixes for your server firmware.

**Power subsystem firmware fixes**
Power subsystem firmware is the code that enables the power subsystem hardware in the 59*x* model servers. Use the information in this section to download, install, and manage fixes for your power subsystem firmware.

**I/O adapter and device firmware fixes**
I/O adapter and device firmware is the code that enables hardware such as Ethernet PCI adapters or disk drives. Use the information in this section to download and install fixes for your I/O adapter and device firmware.

**Operating system fixes**
Use the information in this section to learn how to download and install fixes for your operating systems.

## HMC fixes

Fixes are periodically released for the HMC.

To download and install HMC machine code fixes, follow these steps:

1. Determine the existing level of HMC machine code.
   a. In the Navigation Area, open Licensed Internal Code Maintenance.
   b. Select **HMC Code Update**.
   c. In the right pane, look for the version and release of your HMC machine code in the Status area.
2. Determine the available levels of HMC machine code.

   You need to know if new HMC machine code fixes are available for your machine code release.

   To find out about available levels of HMC machine code fixes, do one of the following:
   - Contact your service provider.
   - Go to Fix Central . From the Web site, click the appropriate family in the **Server** list, click **Hardware Management Console** in the **Product or fix type** list, and click **Continue**.
3. Get HMC fixes.

   You can get HMC fixes in several ways, depending on how your HMC is set up.

   Read about each of the following methods to get the HMC fixes, and choose one of the methods:
   - **Order optical media (CD-ROM).**
     Contact your service provider to order optical media (CD-ROM) with the fixes you need. After you order and receive the optical media, go to the next step.
   - **Download and install fixes from the Internet.**
     To use this method, your HMC must be connected to an open network, and your HMC must have

FTP access to the Internet. This method enables you to download and install fixes in one step using the HMC interface. If you choose to use this method, go to the next step.

- **Download fixes from a Web site to an FTP server that can accept an FTP request from your HMC.**
  To use this method, your HMC must be connected to an open network. This method requires two steps. First, you go to a Web site from which you download the fixes to an FTP server. For example, if your PC has access to the Internet, you might use your PC to download the fixes from the Web site to a directory on your PC. Second, you use the HMC interface to install the fixes from the FTP server (in this example, your PC) to the HMC.

  To download the HMC machine code fixes from the Web site, go to Fix Central, click the appropriate family in the **Server** list, click **Hardware Management Console** in the **Product or fix type** list, and click **Continue**. After you download the fixes from the Web site to your FTP server, go to the next step.

4. Back up the HMC.

   Before you install the fixes, you should back up critical console information on your HMC. For instructions, see back up your HMC.

5. Install fixes.

   To install the fix, follow these steps:

   a. In the navigation area, open Licensed Internal Code Maintenance.

   b. Select **HMC Code Update**.

   c. Select **Install Corrective Service**. *Corrective service* refers to the HMC machine code fix.

   d. On the Install Corrective Service window, select whether you want to install the fix from optical media or download and install the fix from a remote system. The remote system might be one of your FTP servers or a specific system that is available on your service provider's Web site.

      Choose to download the fixes from a remote system in either of these situations:

      - You previously downloaded the fix to one of your FTP servers, and now you want to download the fix to the HMC.

        In this case, specify the following information:

        – Remote site — The fully-qualified host name of the FTP server to which you previously downloaded the patch file (zip file) that contains the fix.

        – Patch file — The name of the patch file (zip file) you downloaded to the FTP server.

        – User ID — Your user ID for the FTP server.

        – Password — Your password for the FTP server.

      - Your HMC has direct access to the Internet, and you want to download and install the fixes directly from the service provider's Web site to your HMC.

        In this case, specify the following information:

        – Remote site — `techsupport.services.ibm.com`

        – Patch file — The name of the patch file (zip file) that resides on the remote site. The name of the patch file changes with each new fix. To find the name of the patch file, go to Hardware Management Console.

        – User ID — `anonymous`

        – Password — Your e-mail address

   e. Click **OK**.

   f. Follow the instructions to install the fixes.

   g. Reboot the HMC for the fixes to take effect.

6. Verify new level of HMC machine code.

   a. In the Navigation Area, open Licensed Internal Code Maintenance.

   b. Select **HMC Code Update**.

c. In the right pane, look for the version and release of your HMC machine code in the Status area. Verify that the version and release match the fix you installed.

## Server firmware fixes

Server firmware is the part of the Licensed Internal Code that enables hardware, such as the service processor. As with other software, your server firmware sometimes requires a fix. You should check for available server firmware fixes regularly and download and install the fixes if necessary.

Depending on your service environment, you can download, install, and manage your server firmware fixes using different interfaces and methods. For example, if you use an HMC to manage your server, you can use the HMC interface to download, install, and manage your server firmware fixes. If you do not use an HMC to manage your server, you can use the functions specific to your operating system to work with server firmware fixes.

**Note:** If you use an HMC to manage your system and you are setting up the server for the first time or upgrading to a new server firmware release, it is recommended that you install the HMC fixes before you install the server firmware fixes.

Use the following information to learn more about server firmware fixes:

- Concepts and terms
  Learn about concepts related to server firmware fixes.
- Scenarios: Server firmware fixes
  Use these scenarios to learn how to download and install server firmware fixes, either through the HMC or through the operating system.
- Manage server firmware fixes
  Learn about tasks you can perform to manage your server firmware fixes.

**Concepts and terms:** Use the following information to understand concepts and terms related to server firmware fixes:

Repository locations
Learn about the locations from which you can download and install server firmware fixes through the HMC.

Levels of server firmware
Learn about the levels of server firmware that are displayed on the HMC interface, such as current and backup levels, and the levels of server firmware that you can download as fixes to your system.

Temporary side and permanent side of the service processor
Learn about the two sides of the service processor that store the server firmware.

Where to find information about fixes
Learn about where to go to learn whether fixes are available.

*Repository locations:* The HMC enables you to download or access server firmware fixes from several places called *repository locations*. You can specify the repository location through the interface on the HMC. Some factors that influence the repository location from which you get server firmware fixes include the level of server firmware fix you want to download (most recent level or earlier level) and the type of service connection you use (modem or direct Internet connection). Use the following information to help you determine the most appropriate repository location from which you can get the server firmware fix.

**Note:** For instructions on getting server firmware fixes using the HMC, see Scenario: Get server firmware fixes through the HMC.

Using the HMC, you can get server firmware fixes from the following repository locations:

- **IBM service Web site** - An IBM Web site that you can access to download only the most recent (highest) level of server firmware fix. You must use a direct Internet connection to access this Web site.
- **IBM support system** - An IBM system that you can access to download all available levels of server firmware fixes. You can use either a modem or a direct Internet connection to access this system.
- **DVD drive** - The DVD drive on the HMC. You select DVD drive when you install the server firmware fix from optical media.
- **FTP site** - A File Transfer Protocol (FTP) server that holds the server firmware fix. You might select FTP site if you know the fix is on another system.

  For example, the system administrator at the Chicago branch office downloaded the fix to an FTP server at his site yesterday. Today, you want to retrieve the fix from the FTP server so you can download it to the server at your site.

  If you select the FTP site, you need to know the following information:
  - FTP site - The fully qualified host and domain name of the FTP server from which you want to download the fix.
  - User ID - Your user ID for the FTP server.
  - Password - Your password for the FTP server.
  - Directory - The directory on the FTP server that holds the server firmware fix. You can specify the default directory `/opt/ccfw/data`, or you can change the directory path if the fix is in a directory other than the default directory. For example, if you downloaded the fix and copied it to a unique directory on the FTP server, you can specify that directory.
- **Hard drive** - The internal hard disk drive on the HMC. You might select hard drive if you know the fix is on the hard drive.

*Levels of server firmware:* If you use an HMC to manage your server, you can use the HMC interface to view the different levels of server firmware that exist on your server and the levels of server firmware fixes that might be available to download and install.

Use the following information to find out about the levels of server firmware on the server:

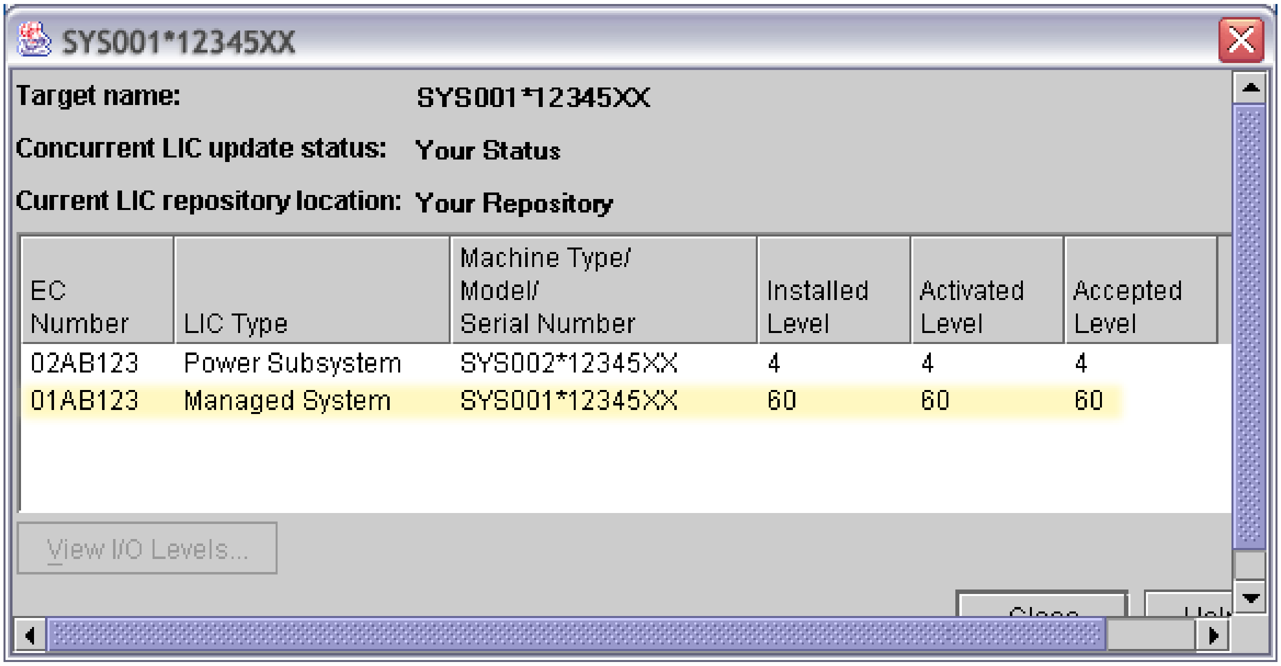
**Existing levels of server firmware**

The server holds the following levels of server firmware:

- **Installed level** - This is the level of server firmware that has been installed and will be loaded into memory after the managed system is powered off and powered on.
- **Activated level** - This is the level of server firmware that is active and running in memory.
- **Accepted level** - This is the backup level of server firmware. You can return to this level of server firmware if you decide to remove the installed level.

The existing levels of server firmware appear on the HMC interface as shown in the highlighted row in the following figure.

**Note:** The values shown in the following figure are used for example purposes only.



SYS001*12345XX

Target name: SYS001*12345XX

Concurrent LIC update status: Your Status

Current LIC repository location: Your Repository

| EC Number | LIC Type | Machine Type/ Model/ Serial Number | Installed Level | Activated Level | Accepted Level |
|---|---|---|---|---|---|
| 02AB123 | Power Subsystem | SYS002*12345XX | 4 | 4 | 4 |
| 01AB123 | Managed System | SYS001*12345XX | 60 | 60 | 60 |

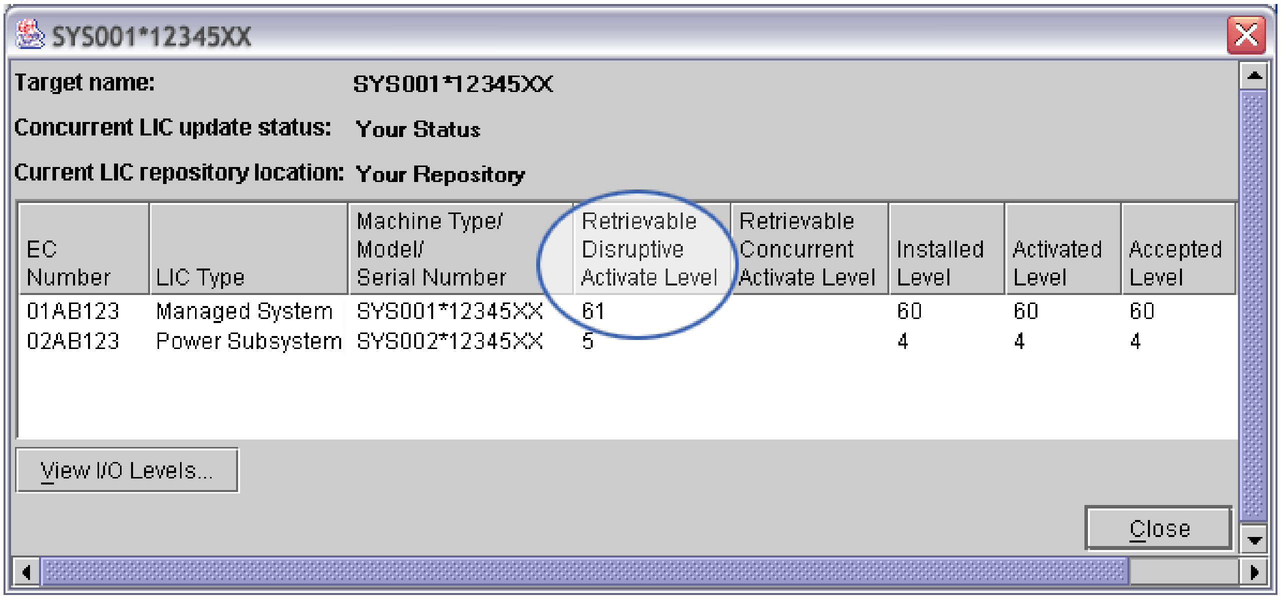
For instructions on how to view the levels of server firmware, see View existing levels of server firmware.

**Available levels of server firmware**

When the service provider issues server firmware fixes, you can view the levels of server firmware (fixes) that can be downloaded and installed from each repository location to your server.

The following figure shows the retrievable level of server firmware and other levels of server firmware. See the detailed descriptions of the retrievable level of server firmware following the figure.

**Note:** The values shown in the following figure are used for example purposes only.



SYS001*12345XX

Target name: SYS001*12345XX

Concurrent LIC update status: Your Status

Current LIC repository location: Your Repository

| EC Number | LIC Type | Machine Type/ Model/ Serial Number | Retrievable Disruptive Activate Level | Retrievable Concurrent Activate Level | Installed Level | Activated Level | Accepted Level |
|---|---|---|---|---|---|---|---|
| 01AB123 | Managed System | SYS001*12345XX | 61 | | 60 | 60 | 60 |
| 02AB123 | Power Subsystem | SYS002*12345XX | 5 | | 4 | 4 | 4 |

- **Retrievable disruptive activate level** - This is the highest level of server firmware available at the selected repository. Activation of this level of server firmware is a disruptive process. Therefore, you will be instructed to shut down all of the applications and logical partitions before initiating the installation, and the managed system will be automatically returned to its original state at the end of the process.
- **Retrievable concurrent activate level** - This is the highest level of server firmware available at the selected repository that can be retrieved, installed, and activated concurrently. Activation of this level of server firmware is a concurrent process. Therefore, it is not necessary to shut down the logical partitions or the managed system before initiating the update, and it is not necessary to power on and off the managed system to activate the fix.

*Temporary side and permanent side of the service processor:* The service processor maintains two copies of the server firmware. One copy is considered the permanent copy and is stored on the permanent side, sometimes referred to as the ″p″ side. The other copy is considered the temporary copy and is stored on the temporary side, sometimes referred to as the ″t″ side. It is recommended that you start and run the server from the temporary side.

When you install a server firmware fix, it is installed on the temporary side.

**Note:** The server firmware fix is installed on the temporary side only after the existing contents of the temporary side are permanently installed on the permanent side. (The service processor performs this process automatically when you install a server firmware fix.) If you want to preserve the contents of the permanent side, you need to remove the current level of firmware (copy the contents of the permanent side to the temporary side) before you install the fix. However, if you get your fixes using **Advanced features** on the HMC interface and you indicate that you do not want the service processor to automatically accept the firmware level, the contents of the temporary side are not automatically installed on the permanent side. In this situation, you do not need to remove the current level of firmware to preserve the contents of the permanent side before you install the fix.

You might want to use the new level of firmware for a period of time to verify that it works correctly. When you are sure that the new level of firmware works correctly, you can permanently install the server firmware fix. When you permanently install a server firmware fix, you copy the temporary firmware level from the temporary side to the permanent side.

Conversely, if you decide that you do not want to keep the new level of server firmware, you can remove the current level of firmware. When you remove the current level of firmware, you copy the firmware level that is currently installed on the permanent side from the permanent side to the temporary side.

To find out how the temporary side and permanent side of the service processor correlate to storage areas A and B in i5/OS, see Install fixes on systems managed by the Hardware Management Console.

*Where to find information about fixes:* As the system administrator, one of your responsibilities is to keep the server firmware up to date. To do that, you need to know when new fixes become available. You can find out about new fixes from the following sources:

- Your service provider
- HMC interface

  The HMC interface enables you to see the levels of server firmware that are currently available for your system. For instructions, see View available levels of server firmware.
- Fix Central

  This Web site enables you to search for server firmware fixes for your specific server. You can order the fixes and download them electronically.

  From the Web site, follow these steps:

  1. In the **Server** list, click the appropriate family. For example, **iSeries family** or **pSeries family**.
  2. In the **Product or fix type** list, click the following:

- For **iSeries family**, click **Server firmware through i5/OS** if you get server firmware fixes through i5/OS. If you use the HMC to get server firmware fixes, see View available levels of server firmware.
- For **pSeries family**, click **Hardware microcode and firmware**.

3. Click **Continue**.

**Scenarios: Server firmware fixes:** These scenarios demonstrate several ways you can download and install server firmware fixes to your system. Use the scenarios to guide you through the process of getting fixes for your server firmware.

**Scenario: Get server firmware fixes with an HMC**
This scenario demonstrates how to use the HMC to download and install the server firmware fixes.

**Scenario: Get server firmware fixes without an HMC**
This scenario demonstrates how to download and install server firmware fixes through your operating system when you do not use an HMC to manage your system.

**Scenario: Get server firmware fixes through i5/OS for an HMC managed system**
This scenario demonstrates how to download and install the server firmware fixes through i5/OS when you use an HMC to manage your system. This method enables you to use the same process to download both your server firmware fixes and i5/OS fixes.

*Scenario: Get server firmware fixes with an HMC:* **Situation**

Suppose you are the system administrator for your company. You use an HMC to manage your server and you have configured several partitions on the server. Periodically, you need to download and install fixes for your server firmware.

You want to use the HMC to perform this task. There are several repository locations from which you can download the fixes using the HMC. For example, you can download the fixes from your service provider’s Web site or support system, from optical media that you order from your service provider, or from an FTP server on which you previously placed the fixes. You can use the interface on the HMC to select any one of these repositories from which you can download and install the server firmware fixes. The Change Internal Code wizard provides a step-by-step process for you to select the appropriate repository and perform the required steps to download and install the fix.

**Objectives**

The objective of this scenario is to use the HMC to download and install the server firmware fix.

**Configuration steps**

You must complete the following tasks:

1. Ensure you have a connection to the service provider.
2. Determine the available levels of server firmware
3. Use the Change Internal Code wizard to update your server firmware.
4. Verify that the fix installed successfully.

*Scenario details: Get server firmware fixes with an HMC:* **Step 1: Ensure you have a connection to the service provider.**

To download server firmware fixes from the service provider’s system or Web site, you need to set up a connection to the service provider either through a local or remote modem or through a VPN connection. You typically set up the service connection when you first set up your server. However, the service connection is not required for initial server setup. Therefore, you need to verify that the service connection exists.

To verify the service connection, follow these steps:

1. In the navigation area, open Service Applications.
2. Select **Remote Support**.
3. Select **Customize Outbound Connectivity**.
4. Select the tab for the type of outbound connectivity you chose for your HMC (Local Modem, Internet VPN, or Pass-Through Systems). For more information about these settings, see Choosing your connection method.

   **Note:** If a connection to the service provider does not exist, you need to set up the service connection before proceeding with this scenario. For instructions on how to set up a connection to the service provider, see Scenarios: Service and support.
5. Click **Test**.
6. Verify that the test completes successfully. If the test is not successful, you need to troubleshoot your connectivity and correct the problem before proceeding with this scenario.

**Step 2: (Optional) Determine the available levels of server firmware**

This step is optional because it is not necessary to determine the available levels of server firmware before downloading and installing new fixes. The Change Internal Code wizard checks the available levels for you and by default installs the highest concurrent level of server firmware fix. If no server firmware fixes are currently available for your server, a message is displayed that indicates no fixes are available.

However, if you want to check the available levels before you download and install the fixes, you can perform this step. Then, after you get the fix, you can verify that the correct level of server firmware was installed.

If you do not want to check the available levels of server firmware, skip to Step 3.

To determine the available levels of server firmware for the managed system, follow these steps:

**Note:** The HMC interface refers to *server firmware* as *Licensed Internal Code*.

1. Expand the **Licensed Internal Code Maintenance** folder.
2. Click the **Licensed Internal Code Updates** icon.
3. In the Contents area, click **Change Internal Code**.
4. In the Target Object Selection window, click the target system, and click **OK**.
5. In the Change Internal Code window, select **View system information** and click **OK**.
6. In the Specify LIC Repository window, select the repository location from which you want to view available server firmware fixes, and click **OK**. For more information about each of the repositories, click **Help**.

   A window is displayed that shows system information for the target system, including the retrievable levels of server firmware. For details about the system information contained in the table, click **Help**.

**Step 3: Use the Change Internal Code wizard to update your server firmware.**

To use the Change Internal Code wizard to download and install your server firmware, follow these steps:

**Note:** The HMC interface refers to *server firmware* as *Licensed Internal Code*.

1. Expand the **Licensed Internal Code Maintenance** folder.
2. Click the **Licensed Internal Code Updates** icon.
3. In the Contents area, click **Change Internal Code**.

4. In the Target Object Selection window, click the target system, and click **OK**.
5. In the Change Internal Code window, select **Start Change Internal Code wizard**, and click **OK**.
6. In the Specify LIC Repository window, select the repository location from which you want to download the server firmware fixes, and click **OK**. For more information on each of the repository locations, click **Help**.
7. In the Change Internal Code Wizard welcome window, click **Next**.

   **Note:** If no fixes are available, a message is displayed that indicates no fixes are available and targets are up-to-date. In this situation, click **Cancel** to end the task.
8. In the Change Internal Code Wizard window, ensure that **Managed System and Power LIC** is selected, and click **Next**.

   **Note:** If I/O firmware fixes are available, additional windows might be displayed. Follow the instructions in these windows to install the I/O firmware fixes.
9. In the Hardware Management Console License Agreement window, read the agreement and click **Accept**.
10. In the Confirm the Action window, perform the required actions, and click **Finish**.

    If the process is disruptive, the following message is displayed on the HMC interface: `Quiesce any applications currently running on your operating systems for the systems listed below.` In this situation, you need to manually shut down all of the applications and logical partitions to prevent the system from shutting them down abnormally during the process.

    Use the normal procedures to shut down the logical partitions:

    - i5/OS logical partitions
      To shut down i5/OS logical partitions, use the Power Down System (PWRDWNSYS) command from an i5/OS command line (either in a 5250 emulator session on your HMC, or on the Operations Console). For further instructions, see Shutting down i5/OS logical partitions.
    - AIX logical partitions
      For instructions, see Shutting down AIX.
    - Linux logical partitions
      For instructions, see Shutting down Linux.

    At the end of a disruptive process, the managed system automatically returns to its original state.

**Step 4: Verify that the fix installed successfully**

To verify that the server firmware fix installed successfully, follow these steps:

**Note:** The HMC interface refers to *server firmware* as *Licensed Internal Code*.

1. Expand the **Licensed Internal Code Maintenance** folder.
2. Click the **Licensed Internal Code Updates** icon.
3. In the Contents area, click **Change Internal Code**.
4. In the Target Object Selection window, click the target system, and click **OK**. The target is the managed system for which you want to verify the server firmware level.
5. In the Change Internal Code window, select **View system information**, and click **OK**.
6. In the Specify LIC Repository window, select **None**, and click **OK**.

   A window is displayed that shows system information for the target system.
7. Verify that the installed and activated levels of server firmware match the fix that you installed.

*Scenario: Get server firmware fixes without an HMC:* **Situation**

Suppose you are the system administrator for your company. Your server is in its manufacturing default configuration, and you do not use an HMC to manage your server. Periodically, you need to download and install fixes for your server firmware. Because you do not use an HMC to manage your server, you must get your fixes through your operating system. In this situation, you can get server firmware fixes through the operating system regardless of whether your operating system is AIX, Linux, or i5/OS.

**Objectives**

The objective of this scenario is to download and install the server firmware fix through your operating system.

**Configuration steps**

You must complete the following tasks:

**Note:** Installing the server firmware fixes through the operating system is a disruptive (nonconcurrent) process if you are running AIX or Linux on the server. That is, the system is automatically powered off and powered on during the installation process. Therefore you will be instructed to shut down all of your applications before you start to install the server firmware fixes through the operating system.

1. (Optional for i5/OS) Determine the existing level of server firmware.
2. (Optional for i5/OS) Determine the available levels of server firmware.
3. Ensure you have a connection to the service provider.
4. Download and install the server firmware fixes.

*Scenario details: Get server firmware fixes without an HMC:* **Step 1: (Optional for i5/OS) Determine the existing level of server firmware**

**Note:**

If you are using i5/OS, this is an optional step. In most situations, it is unnecessary for you to determine the existing level of server firmware. If you follow a preventive fix maintenance strategy by regularly installing current cumulative PTF packages and HIPER PTF groups, you do not need to monitor the server firmware fix levels. However, if your service provider recommends that you install a specific server firmware fix (PTF) to address a specific problem or to add new function, you can use these instructions to determine whether you already have the specific fix. If your service provider has not directed you to install a specific server firmware fix PTF, go to Step 3.

Use one of the following methods to determine the existing level of server firmware on the server:

- **Advanced Systems Management Interface (ASMI)**
  On the ASMI Welcome pane, view the existing level of server firmware in the upper-right corner below the copyright statement. For example, SF220_005.
- **i5/OS command line**
  View existing levels of server firmware using the same functions as you do to view your PTFs. For more information, see Display fixes information on your server. PTFs for server firmware fixes begin with the prefix `MH`. For example, `MHnnnnn` where nnnnn is the number associated to the specific server firmware fix.
- **AIX command line**

  You must have AIX diagnostics installed on your server to perform this task. AIX diagnostics are installed when you install the AIX operating system on your server. However, it is possible to deselect the diagnostics. Therefore, you need to ensure that the online AIX diagnostics are installed before proceeding with this task.

  At an AIX command line, type

  ```
  lsmcode -r -d sys0
  ```

  The existing levels of server firmware are displayed. For example, you might see output similar to the following:

```
system:SF220_005 (t)  SF220_004 (p)  SF220_005 (t)
```

The following table provides descriptions for each of the server firmware levels displayed in the output.

| Server firmware levels displayed | | |
|---|---|---|
| SF220_005 (t) | SF220_004 (p) | SF220_005 (t) |
| • The installed level.<br>• Also known as the temporary level. | • The backup level.<br>• Also known as the permanent level. | • The activated level.<br>• The level on which the server is currently running. |

- **Linux command line**
  To view existing levels of server firmware, you need to download and unpack the following service tools to your server:
  - Platform Enablement Library — librtas-xxxxx.rpm
  - Service Aids — ppc64-utils-xxxxx.rpm
  - Hardware Inventory — lsvpd-xxxxx.rpm

  where xxxxx represents a specific version of the RPM file.

  To download and unpack the service tools to your server, follow these steps:

  1. Go to IBM eServer Support — Linux on Power .
  2. Click your Linux distributor.
  3. Click the RPM file for the service tool.

     **Note:** Download the service tools in the following order.
     a. Platform Enablement Library — librtas-xxxxx.rpm
     b. Service Aids — ppc64-utils-xxxxx.rpm
     c. Hardware Inventory — lsvpd-xxxxx.rpm

     where xxxxx represents a specific version of the RPM file.

     The File Download window is displayed indicating the name of the RPM file. For example, librtas-1.1–12.ppc64.rpm.
  4. In the File Download window, click **Save**, specify the directory to which you want to download the RPM file, and click **Save**.
  5. To unpack the RPM file that contains the service tool, you need to run the following command at a Linux command line for each RPM file:

     ```
     rpm -Uvh --ignoreos filename.rpm
     ```

     where *filename* is the name of the RPM file that contains the service tool. For example, librtas-1.1–12.ppc64.rpm.

  After downloading the service tools to the server or partition running Linux, type the following at a Linux command line:

  ```
  lsmcode -r -d sys0
  ```

  The existing levels of server firmware are displayed. For example, you might see output similar to the following:

  ```
  system:SF220_005 (t)  SF220_004 (p)  SF220_005 (t)
  ```

  The following table provides descriptions for each of the server firmware levels displayed in the output.

| Server firmware levels displayed | | |
|---|---|---|
| SF220_005 (t) | SF220_004 (p) | SF220_005 (t) |
| • The installed level.<br>• Also known as the temporary level. | • The backup level.<br>• Also known as the permanent level. | • The activated level.<br>• The level on which the server is currently running. |

**Step 2: (Optional for i5/OS) Determine the available levels of server firmware**

**Note:**

> If you are using i5/OS, this is an optional step. In most situations, it is unnecessary for you to determine the available levels of server firmware. If you follow a preventive fix maintenance strategy by regularly installing current cumulative PTF packages and HIPER PTF groups, you do not need to monitor the server firmware fix levels. However, if your service provider recommends that you install a specific server firmware fix (PTF) to address a specific problem or to add new function, you can use this step to determine whether the recommended fix is available. If your service provider has not directed you to install a specific server firmware fix PTF, go to Step 3.

The method you use to determine the available levels of server firmware depends on your operating system or server model:

- **i5/OS**
  If your service provider recommends that you install a specific server firmware fix PTF, you can look for that PTF when you order fixes for i5/OS. PTFs for server firmware fixes begin with the prefix `MH`. For example, `MHnnnnn` where nnnnn is the number associated to the specific server firmware fix.
- **IBM eServer p5**

  To determine the available levels of server firmware, go to the Download microcode Web site, and view the available levels of server firmware for your specific server model.

**Step 3: Ensure you have a connection to the service provider.**

To download server firmware fixes from the service provider, you need to set up a connection to the service provider, either through a local or remote modem or through a VPN connection. You typically set up the service connection when you first set up your server. However, the service connection is not required for initial server setup. Therefore, you need to verify that the service connection exists.

If a connection to the service provider does not exist, you need to set up the service connection before proceeding with this scenario. For instructions on how to set up a connection to the service provider, see Scenarios: Service and support.

**Step 4: Download and install the server firmware fixes**

The method you use to download and install the server firmware fixes depends on your operating system:

- **i5/OS**
  Use the i5/OS PTF installation functions on your service partition to download and install the server firmware fixes. For instructions on how to install the server firmware fixes along with i5/OS fixes, see Order fixes.

  When you shut down the i5/OS service partition to install the server firmware fixes, system reference code D6xx430B or D6xx430A might be displayed for an extended period of time. The `xx` should increment periodically and is a normal part of processing when server firmware fixes are being installed. Allow the server to complete the processing; do not interrupt this process.

- **AIX or Linux**

  To download and install the server firmware fix, follow these steps:

  **Note:** When you install a server firmware fix, it is installed on the temporary side of the service processor. However, the server firmware fix is installed on the temporary side only after the original contents of the temporary side are permanently installed on the permanent side. (The service processor performs this process automatically when you install a server firmware fix.) If you want to preserve the contents of the permanent side, you need to remove the current level of firmware (copy the contents of the permanent side to the temporary side) before you install the fix.

  1. Create a directory on the target server to which you can download the server firmware fix.

     At a command line, type the following:

     ```
     mkdir /tmp/fwupdate
     ```

     **Note:** If the `/tmp/fwupdate` directory already exists, be sure it is empty before proceeding.
  2. Download the server firmware fix from the Internet to the server.
     a. Go to the Download microcode Web site, and follow these steps:
        1) In the `Model` column, find your server model
        2) In the associated `Download` column, click **RPM** to download the server firmware fix to your server.

           The License Agreement for Machine Code is displayed.
        3) Read the License Agreement for Machine Code and click **I have read and understood this license agreement and I agree to abide by its terms** to accept the terms of the agreement.

           The File Download window is displayed indicating the name of the RPM file. For example, 01SF220_006_006.rpm.
        4) In the File Download window, click **Save**, specify the `/tmp/fwupdate` directory, and click **Save**.
        5) Unpack the RPM file to obtain the server firmware fix file. If the RPM file is called 01SF220_006_006.rpm, the server firmware fix file is called 01SF220_006_006. (Note that the server firmware fix file does not have a file extension.)

           To unpack the RPM file, type the following at a command line:

           ```
           rpm -ihv --ignoreos fwlevel.rpm
           ```

           where *fwlevel* is the specific server firmware level, such as 01SF220_006_006.

           **Note:** If you receive a warning that a user or group does not exist, you can ignore it.

           The server firmware fix file will be added to the /tmp/fwupdate directory.
  3. Install the server firmware fix to the temporary side of the server.

     Use one of the following methods to install the server firmware fix to the temporary side of the server, depending on your operating system:

     **Note:** Installing the server firmware fixes through the operating system is a disruptive (nonconcurrent) process if you are running AIX or Linux on the server. That is, the system is automatically powered off and powered on during the installation process. Therefore, you need to shut down all of your applications before proceeding with this step.

     – AIX

       Use one of the following methods to install the server firmware fix to the temporary side of the server:

       **Note:** To perform this task, you must have root user authority.

       - Using the AIX diagnostic service aid

To install the server firmware fix to the temporary side of the server, follow these steps:

a. On the AIX command line, type `diag`.

b. Initialize the terminal type, if requested.

c. On the function selection screen, select **Tasks and Service Aids**.

d. On the task selection screen, scroll to the bottom of the list of options, and select **Update and Manage Flash**.

e. A screen similar to the following is displayed:

```
UPDATE AND MANAGE SYSTEM FLASH

The current permanent system firmware image is SF220_005.
The current temporary system firmware image is SF220_005.
The system is currently booted from the temporary image.

Validate and Update System Firmware
Update System Firmware
Commit the Temporary Image
```

Select **Validate and Update System Firmware**, and press Enter.

- Using the update_flash command

  With the server firmware fix file saved in the /tmp/fwupdate subdirectory, type the following at an AIX command line:

  ```
  cd /tmp/fwupdate
  /usr/lpp/diagnostics/bin/update_flash -f fwlevel
  ```

  where *fwlevel* is the specific server firmware fix file name, such as 01SF220_006_006.

– Linux

**Note:** To perform this task, you must have root user authority.

With the server firmware fix file saved in the /tmp/fwupdate subdirectory, type the following at a Linux command line:

```
cd /tmp/fwupdate
/usr/sbin/update_flash -f fwlevel
```

where *fwlevel* is the specific server firmware fix file name, such as 01SF220_006_006.

During the server firmware installation process, reference codes CA2799FD and CA2799FF are alternately displayed in the control panel. After the installation is complete, the system is automatically powered off and powered on.

4. Verify the installation

At a command line, type:

```
lsmcode -r -d sys0
```

The existing levels of server firmware are displayed. For example, you might see output similar to the following:

```
system:SF220_006 (t)  SF220_005 (p)  SF220_006 (t)
```

The following table provides descriptions for each of the server firmware levels displayed in the output.

| **Server firmware levels displayed** | | |
|---|---|---|
| SF220_006 (t) | SF220_005 (p) | SF220_006 (t) |
| • The installed level.<br>• Also known as the temporary level. | • The backup level.<br>• Also known as the permanent level. | • The activated level.<br>• The level on which the server is currently running. |

Verify that the first level and third level indicated in the output match the level that you installed.

5. (Optional) Install the server firmware fix permanently.

   You might want to use the new level of server firmware for a period of time to verify that it works correctly. When you are sure that the new level of server firmware works correctly, you can permanently install the server firmware fix. Be aware that if you install the server firmware fix permanently (copy the temporary firmware level from the temporary side to the permanent side, so that the temporary and permanent sides contain the same level of firmware), you cannot return to the level that was previously on the permanent side. For instructions about how to install server firmware fixes permanently, see Install server firmware fixes permanently. For information about how the service processor stores server firmware, see Temporary side and permanent side of the service processor.

*Scenario: Get server firmware fixes through i5/OS for an HMC-managed system:* **Situation**

Suppose you are the system administrator for your company. You use an HMC to manage your server and you have configured several partitions on the server. Periodically, you need to download and install fixes for your server firmware. You know you can get the fixes either through the HMC or through the operating system.

In this situation, you want to download and install the server firmware fixes through i5/OS because you also need to download and install some new PTFs for i5/OS. i5/OS allows you to get server firmware fixes and operating system PTFs at the same time.

Your HMC is set up, by default, to download and install the server firmware fixes. Therefore, you need to change the default setting to enable your operating system to download and install the fixes. In addition, you need to ensure that one of your logical partitions is designated to be a service partition.

**Objectives**

The objective of this scenario is to download and install the server firmware fix through i5/OS.

**Configuration steps**

You must complete the following tasks:
1. Designate one of your i5/OS logical partitions to be the service partition.
2. Change the firmware update policy from Hardware Management Console (HMC) to operating system.
3. Ensure you have a connection to the service provider.
4. Download and install the server firmware fixes.

*Scenario details: Get server firmware fixes through i5/OS for an HMC-managed system:* **Step 1: Designate one of your i5/OS logical partitions to be the service partition**

**Note:** If you are using an HMC to manage your server but do not have logical partitions, you do not have to designate a service partition.

1. In the Navigation Area, open **Server and Partition**.
2. Select **Server Management**.
3. In the contents area, right-click the managed system and select **Properties**.
4. In the Service partition field, select the logical partition that you want to designate to be the service partition.
5. Click **OK**.

**Step 2: Change the firmware update policy from Hardware Management Console (HMC) to operating system**

Your HMC is set up, by default, to download and install the server firmware fixes. Therefore, you need to change the default setting in the firmware update policy to enable your operating system to download and install the fixes.

**Note:** Before changing your firmware update policy to operating system, you should be aware of the level of server firmware that is on your managed system and what server firmware is installed on your service partition. For instructions on how to check the level of server firmware on the managed system and service partition, see Display level of fixes.

When you set the firmware update policy to the operating system, the current level of the server firmware portion of the Licensed Internal Code on the service partition is used to update the server firmware that is running on the managed system the next time the service partition is shut down. Consequently, if the server firmware on the service partition is at a lower level than the server firmware running on the managed system, the installation process could install a lower level of server firmware on the managed system the next time the service partition is shut down.

To avoid this situation, you need to ensure that the proper server firmware PTFs are installed on your service partition before you change your firmware update policy to the operating system. The server firmware on the service partition should be at the same or a higher level than the server firmware running on the managed system before you change the firmware update policy to the operating system.

Use one of the following methods to change the firmware update policy:

- **Advanced System Management Interface (ASMI)**
  To use the ASMI to change the firmware update policy from **Hardware Management Console (HMC)** to **Operating System**, see Changing firmware update policy. You can access the ASMI through Service Focal Point in the HMC GUI, or point your browser to the ASMI. You will need the ASMI admin login and password to use these menus.
- **HMC remote command line**
  To change the firmware update policy using the HMC remote command line, specify the `UPDLIC` command. To find out how to work with the HMC remote command line, see Using the remote command line.

  Use the following examples to change the firmware update policy using the `UPDLIC` command:
  - To change the firmware update policy to Operating System, type:

    ```
    updlic -m xxxx -o o
    ```

    where xxxx is either the machine type, model, and serial number or the name of the managed system.
  - To change the firmware update policy to HMC, type:

    ```
    updlic -m xxxx -o h
    ```

    where xxxx is either the machine type, model, and serial number or the name of the managed system.

**Step 3: Ensure you have a connection to the service provider.**

To download server firmware fixes from the service provider, you need to set up a connection to the service provider either through a local or remote modem or through a VPN connection. You typically set up the service connection when you first set up your server. However, the service connection is not required for initial server setup. Therefore, you need to verify that the service connection exists.

To verify the service connection, follow these steps:

1. In the navigation area, open Service Applications.
2. Select **Remote Support**.

3. Select **Customize Outbound Connectivity**.
4. Select the tab for the type of outbound connectivity you chose for your HMC (Local Modem, Internet VPN, or Pass-Through Systems). For more information about these settings, see Choosing your connection method.

   **Note:** If a connection to the service provider does not exist, you need to set up the service connection before proceeding with this scenario. For instructions on how to set up a connection to the service provider, see Scenarios: Service and support.
5. Click **Test**.
6. Verify that the test completes successfully. If the test is not successful, you need to troubleshoot your connectivity and correct the problem before proceeding with this scenario.

**Step 4: Download and install the server firmware fixes**

Use the i5/OS PTF installation functions on your service partition to update the server firmware. For instructions on how to install the server firmware fixes along with the i5/OS fixes, see Order fixes.

When you shut down the i5/OS service partition to install the server firmware fixes, system reference code D6xx430B or D6xx430A might be displayed for an extended period of time. The xx should increment periodically and is a normal part of processing when server firmware fixes are being installed. Allow the server to complete the processing; do not interrupt this process.

**Manage server firmware fixes:** You can manage your server firmware fixes in several ways. Read the following topics for details.

**Note:** For instructions on how to download and install new server firmware fixes, see Scenarios: Server firmware

- **View existing levels of server firmware**
  Find out how to view the level of server firmware that currently runs on your server.
- **View available levels of server firmware**
  Find out how to view the levels of server firmware that are available for you to download as fixes.
- **View server firmware fix cover letter**
  Find out how to view the server firmware fix cover letter.
- **Remove current level of server firmware**
  Find out how to remove the current level of server firmware so you can return to a previous level of server firmware.
- **Get specific server firmware fix**
  Find out how to download and install a specific level of server firmware rather than the highest level of server firmware.
- **Install server firmware fix permanently**
  Find out how to permanently install the server firmware fix.
- **Upgrade to new server firmware release**
  Find out how to upgrade your server firmware to a new release.

*View existing levels of server firmware:* You can view the current and backup levels of server firmware on the managed system. Use one of the following methods to view the existing level of server firmware, depending on your service environment:

**With HMC**

To view the existing levels of server firmware on the managed system, follow these steps:

**Note:** The HMC interface refers to *server firmware* as *Licensed Internal Code*.

1. Expand the **Licensed Internal Code Maintenance** folder.
2. Click the **Licensed Internal Code Updates** icon.
3. In the Contents area, click **Change Internal Code**.
4. In the Target Object Selection window, click the target system, and click **OK**. The target is the managed system for which you want to check the server firmware level.
5. In the Change Internal Code window, select **View system information**, and click **OK**.
6. In the Specify LIC Repository window, select **None**, and click **OK**.

   A window is displayed that shows system information for the target system. The Installed Level indicates the level of server firmware that has been installed and will be loaded into memory after the managed system is powered off and powered on. The Activated Level indicates the level of server firmware that is active and running in memory. The Accepted Level indicates the backup level of server firmware. You can return to the backup level of server firmware if you decide to remove the installed level. For details about the system information contained in the table, click **Help**.

**Without HMC**

If you do not use an HMC to manage your system or you do not want to use an HMC for this task, you can determine the existing levels of server firmware in the following ways:

- **Advanced Systems Management Interface (ASMI)**
  On the ASMI Welcome pane, view the existing level of server firmware in the upper-right corner below the copyright statement. For example, SF220_025.
- **i5/OS command line**

  In most situations, it is unnecessary for you to determine the existing level of server firmware. If you follow a preventive fix maintenance strategy by regularly installing current cumulative PTF packages and HIPER PTF groups, you do not need to monitor the server firmware fix levels.

  However, if your service provider recommends that you install a specific server firmware fix (PTF) to address a specific problem or to add new function, you can use these instructions to determine whether you already have the specific fix.

  View existing levels of server firmware using the same functions as you do to view your PTFs. For more information, see Display fixes information on your server. PTFs for server firmware fixes begin with the prefix `MH`. For example, `MHnnnnn` where nnnnn is the number associated to the specific server firmware fix.
- **AIX command line**

  You must have AIX diagnostics installed on your server to perform this task. AIX diagnostics are installed when you install the AIX operating system on your server. However, it is possible to deselect the diagnostics. Therefore, you need to ensure that the online AIX diagnostics are installed before proceeding with this task.

  At an AIX command line, type

  ```
  lsmcode -r -d sys0
  ```

  The existing levels of server firmware are displayed. For example, you might see output similar to the following:

  ```
  system:SF220_026 (t)  SF220_025 (p)  SF220_026 (t)
  ```

  The following table provides descriptions for each of the server firmware levels displayed in the output.

| Server firmware levels displayed | | |
|---|---|---|
| SF220_026 (t) | SF220_025 (p) | SF220_026 (t) |

| Server firmware levels displayed | | |
|---|---|---|
| • The installed level.<br>• Also known as the temporary level. | • The backup level.<br>• Also known as the permanent level. | • The activated level.<br>• The level on which the server is currently running. |

- **Linux command line**
  To view existing levels of server firmware, you need to download and unpack the following service tools to your server:
  - Platform Enablement Library — librtas-xxxxx.rpm
  - Service Aids — ppc64-utils-xxxxx.rpm
  - Hardware Inventory — lsvpd-xxxxx.rpm

  where xxxxx represents a specific version of the RPM file.

  To download and unpack the service tools to your server, follow these steps:

  1. Go to IBM eServer Support — Linux on Power .
  2. Click your Linux distributor.
  3. Click the RPM file for the service tool.

     **Note:** Download the service tools in the following order.
     a. Platform Enablement Library — librtas-xxxxx.rpm
     b. Service Aids — ppc64-utils-xxxxx.rpm
     c. Hardware Inventory — lsvpd-xxxxx.rpm

     where xxxxx represents a specific version of the RPM file.

     The File Download window is displayed indicating the name of the RPM file. For example, librtas-1.1–12.ppc64.rpm.
  4. In the File Download window, click **Save**, specify the directory to which you want to download the RPM file, and click **Save**.
  5. To unpack the RPM file that contains the service tool, you need to run the following command at a Linux command line for each RPM file:

     ```
     rpm -Uvh --ignoreos filename.rpm
     ```

     where *filename* is the name of the RPM file that contains the service tool. For example, librtas-1.1–12.ppc64.rpm.

  After downloading the service tools to the server, type the following at a Linux command line:

  ```
  lsmcode -r -d sys0
  ```

  The existing levels of server firmware are displayed. For example, you might see output similar to the following:

  ```
  system:SF220_026 (t)  SF220_025 (p)  SF220_026 (t)
  ```

  The following table provides descriptions for each of the server firmware levels displayed in the output.

| Server firmware levels displayed | | |
|---|---|---|
| SF220_026 (t) | SF220_025 (p) | SF220_026 (t) |
| • The installed level.<br>• Also known as the temporary level. | • The backup level.<br>• Also known as the permanent level. | • The activated level.<br>• The level on which the server is currently running. |

*View available levels of server firmware:* Use one of the following methods to view the available levels of server firmware fixes, depending on your service environment:

**With HMC**

To view the available levels of server firmware for the managed system using the HMC, follow these steps:

**Note:** The HMC interface refers to *server firmware* as *Licensed Internal Code*.

1. Expand the **Licensed Internal Code Maintenance** folder.
2. Click the **Licensed Internal Code Updates** icon.
3. In the Contents area, click **Change Internal Code**.
4. In the Target Object Selection window, click the target system, and click **OK**.
5. In the Change Internal Code window, select **View system information** and click **OK**.
6. In the Specify LIC Repository window, select the repository location from which you want to view available server firmware fixes, and click **OK**. For more information on each of the repositories, click **Help**.

   A window is displayed that shows system information for the target system, including the retrievable levels of server firmware. For details about the system information contained in the table, click **Help**.

   **Note:** If no server firmware fixes are available at the selected repository, the columns in the table will be empty.

**Without HMC**

If you do not use an HMC to manage your system or you do not want to use an HMC for this task, you can determine the available levels of server firmware in the following ways:

- **i5/OS**

  In most situations, it is unnecessary for you to determine the available levels of server firmware. If you follow a preventive fix maintenance strategy by regularly installing current cumulative PTF packages and HIPER PTF groups, you do not need to monitor the server firmware fix levels.

  However, if your service provider recommends that you install a specific server firmware fix (PTF) to address a specific problem or to add new function, you can use this step to determine whether the recommended fix is available.

  If your service provider recommends that you install a specific server firmware fix PTF, you can look for that PTF when you order fixes for i5/OS. PTFs for server firmware fixes begin with the prefix `MH`. For example, `MHnnnnn` where nnnnn is the number associated to the specific server firmware fix.
- **IBM eServer p5**

  To view the available levels of server firmware for the managed system, follow these steps:

  1. Go to Fix Central .
  2. In the **Server** list, click **pSeries family**.
  3. In the **Product or fix type** list, click **Hardware microcode and firmware**.
  4. Click **Continue**.

*View server firmware fix cover letter:* Server firmware fixes can correct known problems or add new function to the code in your current server firmware release. To find out what problems the server firmware fix will correct, or to find out what new function is included in the server firmware fix, you can view the server firmware fix cover letter.

Use one of the following methods to view the server firmware fix cover letter, depending on your service environment:

**With HMC**

To view the server firmware fix cover letter, follow these steps:

1. Expand the **Licensed Internal Code Maintenance** folder.
2. Click the **Licensed Internal Code Updates** icon.
3. In the Contents area, click **Change Internal Code**.
4. In the Target Object Selection window, click the target system, and click **OK**.
5. In the Change Internal Code window, select **Start Change Internal Code wizard**, and click **OK**.
6. In the Specify LIC Repository window, select the repository location from which you want to view the fix cover letter, and click **OK**. For more information about each of the repositories, click **Help**.
7. In the Change Internal Code Wizard welcome window, click **Next**.

   **Note:** If no fixes are available, a message is displayed that indicates no fixes are available and targets are up-to-date. In this situation, click **Cancel** to end the task.
8. In the Change Internal Code Wizard window, ensure that **Managed System and Power LIC** is selected, and click **Advanced Options...**.

   **Note:** If I/O firmware fixes are available, an additional window might be displayed.
9. In the Managed System and Power Licensed Internal Code (LIC) Concurrency window, select the managed system, and click **View information**.
10. In the Managed System and Power Licensed Internal Code (LIC) Level Details window, select the LIC Type for which you want to view the server firmware fix cover letter, and click **View Details**. For example, you might select **Managed System**.

    The server firmware fix cover letter is displayed. Read the cover letter to learn about what problems the server firmware fix will correct, or to find out what new function is included in the server firmware fix.

**Without HMC**

If you do not use an HMC to manage your system or you do not want to use an HMC for this task, you can view the server firmware fix cover letter in different ways, depending on your operating system:

- i5/OS
  For instructions, see Display and print fix cover letters. To view the server firmware fix cover letter, you need to identify the PTFs that correspond to the server firmware fixes. PTFs for server firmware fixes begin with the prefix `MH`. For example, `MHnnnnn` where nnnnn is the number associated to the specific server firmware fix.
- AIX and Linux
  You can view server firmware fix cover letters in several places. For example, you can download cover letters from Web sites, or you can read cover letters that accompany optical media. Contact your service provider for more information.

*Get specific server firmware fix:* You can download and install a specific level of server firmware rather than the highest (most recent) level fix.

Use one of the following methods to download and install a specific server firmware fix, depending on your service environment:

**With HMC**

**Note:** The HMC interface refers to *server firmware* as *Licensed Internal Code*. Similarly, the HMC interface refers to *server firmware fix* as *Licensed Internal Code level*.

To get a specific server firmware fix, follow these steps:

1. Expand the **Licensed Internal Code Maintenance** folder.
2. Click the **Licensed Internal Code Updates** icon.
3. In the Contents area, click **Change Internal Code**.
4. In the Target Object Selection window, click the target system, and click **OK**.
5. In the Change Internal Code window, select **Select advanced features**, and click **OK**.
6. In the Advanced features window, select **Install and activate (implied retrieve)**, and click **OK**.
7. In the Specify LIC Repository window, select the repository location from which you want to download and install the specific server firmware fix, and click **OK**. For more information about each of the repositories, click **Help**.
8. In the Install and Activate (Implied Retrieve) window, select **Specific levels** for LIC level type, and click **OK**.
9. In the Specify LIC Levels window, select the LIC type for which you want to choose a specific level, and click **Change Level...**. For example, you might select **Managed system**.
   - In the Select LIC Level window, select the LIC level you want to install, and click **OK**. Select **None** if you do not want to update the selected LIC type.

     The Specify LIC Levels window is displayed again, showing the LIC type and LIC level that you selected.
   - In the Specify LIC Levels window, verify that the LIC type and LIC level displayed are correct, and click **OK**.
10. This step applies only if the process is disruptive. In the Select Installation Type window, select **Concurrent install only, with deferred disruptive activate** if you want to install the server firmware fix now and activate the server firmware fix later, or select **Disruptive install and activate** if you want to install and activate the server firmware level immediately, and click **OK**.
11. In the Hardware Management Console License Agreement window, read the agreement and click **Accept**.
12. In the Confirm the Action window, perform the required actions, and click **OK**.

    If the process is disruptive, the following message is displayed on the HMC interface: `Quiesce any applications currently running on your operating systems for the systems listed below.` In this situation, you need to manually shut down all of the applications and logical partitions to prevent the system from shutting them down abnormally.

    Use the normal procedures to shut down the logical partitions:
    - i5/OS logical partitions
      To shut down i5/OS logical partitions, use the Power Down System (PWRDWNSYS) command from an i5/OS command line (either in a 5250 emulator session on your HMC, or on the Operations Console). For further instructions, see Shutting down i5/OS logical partitions.
    - AIX logical partitions
      For instructions, see Shutting down AIX.
    - Linux logical partitions
      For instructions, see Shutting down Linux.

    At the end of a disruptive process, the managed system automatically returns to its original state.

**Without HMC**

If you do not use an HMC to manage your system or you do not want to use an HMC for this task, you can get a specific server firmware fix in different ways, depending on your operating system:

- **i5/OS**
  Use the i5/OS PTF installation functions on your service partition to update the server firmware. For instructions on how to install the server firmware fixes along with i5/OS fixes, see Order fixes.
- **AIX or Linux**

  1. Go to Fix Central .

2. In the **Server** list, click **pSeries family**.
3. In the **Product or fix type** list, click **Hardware microcode and firmware**.
4. Click **Continue**.

*Install server firmware fix permanently:* After you download and install a server firmware fix, the fix is temporarily installed until you install it permanently. You might want to use the new level of server firmware for a period of time to verify that it works correctly. When you are sure that the new level of server firmware works correctly, you can permanently install the server firmware fix. Be aware that if you install the server firmware fix permanently (copy the temporary firmware level from the temporary side to the permanent side, so that the temporary and permanent sides contain the same level of firmware), you cannot return to the level that was previously on the permanent side.

**Note:** You might recognize the process of installing the server firmware fix permanently by different terms, depending on the type of hardware or software you use. For example, if you use AIX or Linux, you might refer to this process as *committing* the fix. If you use i5/OS, you refer to this process as *applying* the fix. If you use an HMC, you might refer to this process as *accepting* the fix.

Use one of the following methods to permanently install the server firmware fix, depending on your service environment:

**With HMC**

**Note:** The HMC interface refers to *server firmware* as *Licensed Internal Code*.

To permanently install the server firmware fix, follow these steps:
1. Expand the **Licensed Internal Code Maintenance** folder.
2. Click the **Licensed Internal Code Updates** icon.
3. In the Contents area, click **Change Internal Code**.
4. In the Target Object Selection window, click the target system, and click **OK**. The target is the managed system on which you want to permanently install the server firmware fix.
5. In the Change Internal Code window, select **Select advanced features** and click **OK**.
6. In the Advanced Features window, select **Accept**, and click **OK**.
7. In the Confirm the Action window, click **OK**.

**Without HMC**

If you do not use an HMC to manage your system or you do not want to use an HMC for this task, you can permanently install the server firmware fix in different ways, depending on the operating system you use to download and install the server firmware fix:

- **i5/OS**

  To permanently install the server firmware fix, you need to identify the PTFs that correspond to the server firmware fixes. PTFs for server firmware fixes begin with the prefix `MH`. For example, `MHnnnnn` where nnnnn is the number associated to the specific server firmware fix. For instructions about how to permanently install the server firmware fix, see Advanced fix installation: Apply fixes.
- **AIX**

  Use one of the following methods to permanently install the server firmware fix:

  **Note:** To perform this task, you must have root user authority, and you must start your server from the temporary side.

  – Using the AIX diagnostic service aid

    To permanently install the server firmware fix, follow these steps:

    1. On the AIX command line, type `diag`.

    2. Initialize the terminal type, if requested.
    3. On the function selection screen, select **Tasks and Service Aids**.
    4. On the task selection screen, scroll to the bottom of the list of options, and select **Update and Manage Flash**.
    5. A screen similar to the following is displayed:

       ```
       UPDATE AND MANAGE SYSTEM FLASH

       The current permanent system firmware image is SF220_025.
       The current temporary system firmware image is SF220_026.
       The system is currently booted from the temporary image.

       Validate and Update System Firmware
       Update System Firmware
       Commit the Temporary Image
       ```

       Select **Commit the Temporary Image**, and press Enter. The process might run for ten or more minutes.
    6. Use the manual process to shut down and restart the server.
  - Using the update_flash command

    To permanently install the server firmware fix, follow these steps:

    1. At an AIX command line, type the following:

       ```
       /usr/lpp/diagnostics/bin/update_flash -c
       ```

       The update_flash -c command might run for ten or more minutes.
    2. Use the manual process to shut down and restart the server.

- **Linux**

  **Note:** To perform this task, you must have root user authority, and you must start your server from the temporary side.

  To permanently install the server firmware fix, you need to download and unpack the following service tools to your server:

  - Platform Enablement Library — librtas-xxxxx.rpm
  - Service Aids — ppc64-utils-xxxxx.rpm

  where xxxxx represents a specific version of the RPM file.

  To download and unpack the service tools to your server, follow these steps:

  1. Go to IBM eServer Support — Linux on Power .
  2. Click your Linux distributor.
  3. Click the RPM file for the service tool.

     **Note:** Download the service tools in the following order.

     a. Platform Enablement Library — librtas-xxxxx.rpm

     b. Service Aids — ppc64-utils-xxxxx.rpm

     where xxxxx represents a specific version of the RPM file.

     The File Download window is displayed indicating the name of the RPM file. For example, librtas-1.1–12.ppc64.rpm.
  4. In the File Download window, click **Save**, specify the directory to which you want to download the RPM file, and click **Save**.
  5. To unpack the RPM file that contains the service tool, you need to run the following command at a Linux command line for each RPM file:

     ```
     rpm -Uvh --ignoreos filename.rpm
     ```

where *filename* is the name of the RPM file that contains the service tool. For example, librtas-1.1–12.ppc64.rpm.

After you install the service tools, follow these steps:

1. At a Linux command line, type the following:

   ```
   /usr/sbin/update_flash -c
   ```

   The update_flash -c command might run for ten or more minutes.
2. Use the manual process to shut down and restart the server.

*Remove current level of server firmware:* You can remove the current level of server firmware if you want to return to a previous level of server firmware. Use one of the following methods to remove the current level of server firmware, depending on your service environment:

**With HMC**

**Note:** The HMC interface refers to *server firmware* as *Licensed Internal Code*.

To remove the current level of server firmware, follow these steps:

1. Expand the **Licensed Internal Code Maintenance** folder.
2. Click the **Licensed Internal Code Updates** icon.
3. In the Contents area, click **Change Internal Code**.
4. In the Target Object Selection window, click the target system, and click **OK**. The target is the managed system from which you want to remove the current level of server firmware.
5. In the Change Internal Code window, select **Select advanced features** and click **OK**.
6. In the Advanced Features window, select **Remove and activate**, and click **OK**.
7. In the Confirm the Action window, perform the required actions, and click **OK**.

   If the process is disruptive, the following message is displayed on the HMC interface: `Quiesce any applications currently running on your operating systems for the systems listed below.` In this situation, you need to manually shut down all of the applications and logical partitions to prevent the system from shutting them down abnormally.

   Use the normal procedures to shut down the logical partitions:

   - i5/OS logical partitions
     To shut down i5/OS logical partitions, use the Power Down System (PWRDWNSYS) command from an i5/OS command line (either in a 5250 emulator session on your HMC, or on the Operations Console). For further instructions, see Shutting down i5/OS logical partitions.
   - AIX logical partitions
     For instructions, see Shutting down AIX.
   - Linux logical partitions
     For instructions, see Shutting down Linux.

   At the end of a disruptive process, the managed system automatically returns to its original state.

**Without HMC**

If you do not use an HMC to manage your system or you do not want to use an HMC for this task, you can remove the current level of server firmware in different ways, depending on the operating system you use to download and install the server firmware fix:

- **i5/OS**

  To remove the current level of server firmware, you need to identify the PTFs that correspond to the server firmware fixes. PTFs for server firmware fixes begin with the prefix `MH`. For example, `MHnnnnn` where nnnnn is the number associated to the specific server firmware fix. For instructions about how to remove the server firmware PTFs, see Remove i5/OS fixes.

When you shut down the i5/OS service partition to install the server firmware fixes, system reference code D6xx430B or D6xx430A might be displayed for an extended period of time. The xx should increment periodically and is a normal part of processing when server firmware fixes are being installed. Allow the server to complete the processing; do not interrupt this process.

- **AIX**

  Use one of the following methods to remove the current level of server firmware:

  **Note:** To perform this task, you must have root user authority, and you must start your server from the permanent side.

  - Using the AIX diagnostic service aid

    To remove the current level of server firmware, follow these steps:

    1. On the AIX command line, type `diag`.
    2. Initialize the terminal type, if requested.
    3. On the function selection screen, select **Tasks and Service Aids**.
    4. On the task selection screen, scroll to the bottom of the list of options, and select **Update and Manage Flash**.
    5. A screen similar to the following is displayed:

       ```
       UPDATE AND MANAGE SYSTEM FLASH

       The current permanent system firmware image is SF220_025.
       The current temporary system firmware image is SF220_026.
       The system is currently booted from the permanent image.

       Validate and Update System Firmware
       Update System Firmware
       Reject the Temporary Image
       ```

       Select **Reject the Temporary Image**, and press Enter.

  - Using the update_flash command

    To remove the current level of server firmware, type the following at an AIX command line:

    ```
    /usr/lpp/diagnostics/bin/update_flash -r
    ```

- **Linux**

  **Note:** To perform this task, you must have root user authority, and you must start your server from the permanent side.

  To remove the current level of server firmware, you need to download and unpack the following service tools to your server:

  - Platform Enablement Library — librtas-xxxxx.rpm
  - Service Aids — ppc64-utils-xxxxx.rpm

  where xxxxx represents a specific version of the RPM file.

  To download and unpack the service tools to your server, follow these steps:

  1. Go to IBM eServer Support — Linux on Power .
  2. Click your Linux distributor.
  3. Click the RPM file for the service tool.

     **Note:** Download the service tools in the following order.

     a. Platform Enablement Library — librtas-xxxxx.rpm

     b. Service Aids — ppc64-utils-xxxxx.rpm

     where xxxxx represents a specific version of the RPM file.

   The File Download window is displayed indicating the name of the RPM file. For example, librtas-1.1–12.ppc64.rpm.
4. In the File Download window, click **Save**, specify the directory to which you want to download the RPM file, and click **Save**.
5. To unpack the RPM file that contains the service tool, you need to run the following command at a Linux command line for each RPM file:

   ```
   rpm -Uvh --ignoreos filename.rpm
   ```

   where *filename* is the name of the RPM file that contains the service tool. For example, librtas-1.1–12.ppc64.rpm.

After you install the service tools, type the following at a Linux command line:

```
/usr/sbin/update_flash -r
```

*Upgrade to new server firmware release:* Use one of the following methods to upgrade your server firmware to a new release, depending on your service environment:

**With HMC**

**Note:** The HMC interface refers to *server firmware* as *Licensed Internal Code*.

To upgrade to a new server firmware release, follow these steps:
1. Obtain optical media that contains the new server firmware release from your service provider.
2. Insert optical media into the drive on the HMC.
3. Expand the **Licensed Internal Code Maintenance** folder.
4. Click the **Licensed Internal Code Updates** icon.
5. In the Contents area, click **Manufacturing Equipment Specification Upgrade**.
6. In the **Target Object Selection** window, click the target system, and click **OK**. The target is the managed system for which you want to upgrade the server firmware to a new release.
7. In the Hardware Management Console License Agreement window, read the agreement and click **Accept**.
8. In the **Manufacturing Equipment Specification Upgrade — Confirm the Action** window, perform any required actions, and click **OK**.

   The following message might be displayed on the HMC interface: `Quiesce any applications currently running on your operating systems for the systems listed below.` In this situation, you need to manually shut down all of the applications and logical partitions to prevent the system from shutting them down abnormally.

   Use the normal procedures to shut down the logical partitions:
   - i5/OS logical partitions
     To shut down i5/OS logical partitions, use the Power Down System (PWRDWNSYS) command from an i5/OS command line (either in a 5250 emulator session on your HMC, or on the Operations Console). For further instructions, see Shutting down i5/OS logical partitions.
   - AIX logical partitions
     For instructions, see Shutting down AIX.
   - Linux logical partitions
     For instructions, see Shutting down Linux.

   At the end of a disruptive process, the managed system automatically returns to its original state.

**Without HMC**

If you do not use an HMC to manage your system, you can upgrade to a new server firmware release by downloading and installing the new server firmware release through your operating system, as follows:

- i5/OS
  Use the normal PTF install functions on your service partition to upgrade to a new server firmware release. For instructions, see Order fixes. When you order server firmware fixes, you automatically receive the PTFs for the latest server firmware release that is available.

  When you shut down the i5/OS service partition to install the server firmware fixes, system reference code D6xx430B or D6xx430A might be displayed for an extended period of time. The xx should increment periodically and is a normal part of processing when server firmware fixes are being installed. Allow the server to complete the processing; do not interrupt this process.
- AIX
  Contact your service provider.
- Linux
  Contact your service provider.

## Power subsystem firmware fixes

Power subsystem firmware is the part of the Licensed Internal Code that enables the power subsystem hardware in the 59*x* model servers. As with other software, your power subsystem firmware sometimes requires a fix.

Use the following information to learn more about power firmware fixes:

- Concepts and terms
  Learn about concepts related to power subsystem firmware fixes.
- Scenarios: Power subsystem firmware fixes
  Use these scenarios to learn how to download and install power subsystem firmware fixes.
- Manage power subsystem firmware fixes
  Learn about tasks you can perform to manage your power subsystem firmware fixes.

**Concepts and terms:** Use the following information to understand concepts and terms related to power subsystem firmware fixes:

Repository locations
Learn about the locations from which you can download and install power subsystem firmware fixes through the HMC.

Levels of power subsystem firmware
Learn about the levels of power subsystem firmware that are displayed on the HMC interface, such as current and backup levels, and the levels of power subsystem firmware that you can download as fixes to your system.

*Repository locations:* The HMC enables you to download or access power subsystem firmware fixes from several places called *repository locations*. You can specify the repository location through the interface on the HMC. Some factors that influence the repository location from which you get power subsystem firmware fixes include the level of power subsystem firmware fix you want to download (most recent level or earlier level) and the type of service connection you use (modem or direct Internet connection). Use the following information to help you determine the most appropriate repository location from which you can get the power subsystem firmware fix.

**Note:** For instructions on getting power subsystem firmware fixes using the HMC, see Scenario: Get power subsystem firmware fixes through the HMC.

Using the HMC, you can get power subsystem firmware fixes from the following repository locations:

- **IBM service Web site** - An IBM Web site that you can access to download only the most recent (highest) level of power subsystem firmware fix. You must use a direct Internet connection to access this Web site.

- **IBM support system** - An IBM system that you can access to download all available levels of power subsystem firmware fixes. You can use either a modem or a direct Internet connection to access this system.
- **DVD drive** - The DVD drive on the HMC. You select DVD drive when you install the power subsystem firmware fix from optical media.
- **FTP site** - A File Transfer Protocol (FTP) server that holds the power subsystem firmware fix. You might select FTP site if you know the fix is on another system.

  For example, the system administrator at the Chicago branch office downloaded the fix to an FTP server at his site yesterday. Today, you want to retrieve the fix from the FTP server so you can download it to the server at your site.

  If you select the FTP site, you need to know the following information:
  - FTP site - The fully qualified host and domain name of the FTP server from which you want to download the fix.
  - User ID - Your user ID for the FTP server.
  - Password - Your password for the FTP server.
  - Directory - The directory on the FTP server that holds the power subsystem firmware fix. You can specify the default directory `/opt/ccfw/data`, or you can change the directory path if the fix is in a directory other than the default directory. For example, if you downloaded the fix and copied it to a unique directory on the FTP server, you can specify that directory.
- **Hard drive** - The internal hard disk drive on the HMC. You might select hard drive if you know the fix is on the hard drive.

*Levels of power subsystem firmware:* You can use the HMC interface to view the different levels of power subsystem firmware that exist on your server and the levels of power subsystem firmware fixes that might be available to download and install.

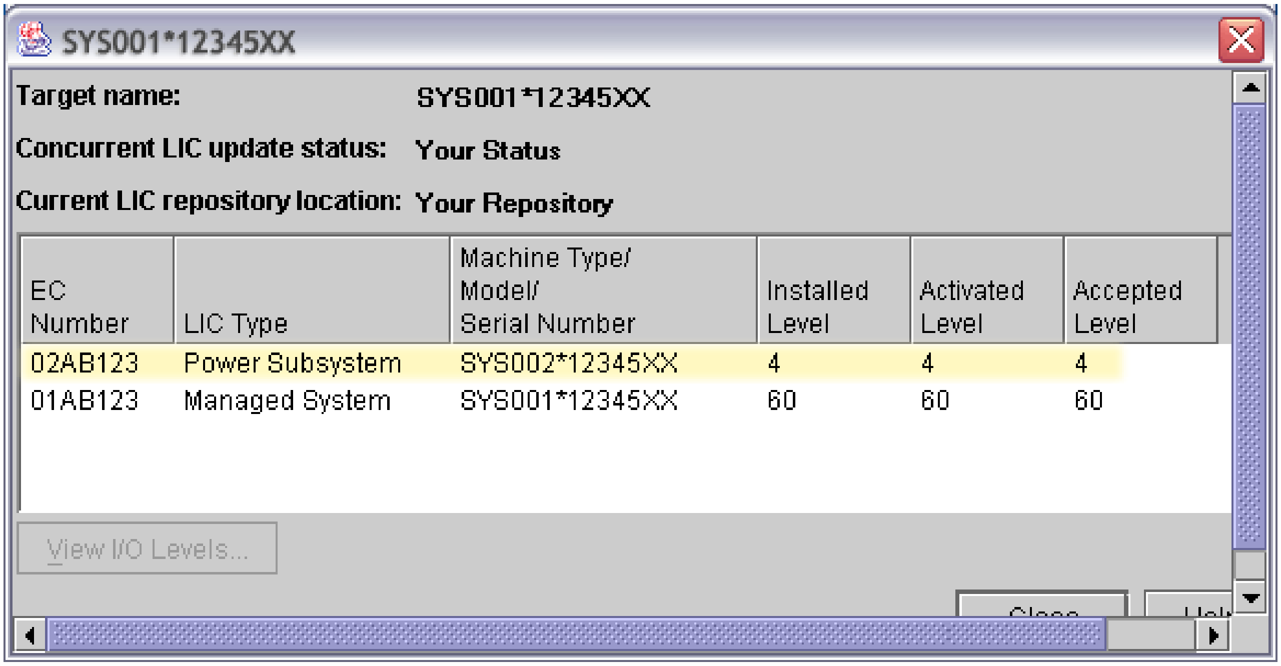
Use the following information to find out about the levels of power subsystem firmware on the server:

**Existing levels of power subsystem firmware**

The server holds the following levels of power subsystem firmware:
- **Installed level** - This is the level of power subsystem firmware that has been installed and will be loaded into memory after the managed system is powered off and powered on.
- **Activated level** - This is the level of power subsystem firmware that is active and running in memory.
- **Accepted level** - This is the backup level of power subsystem firmware. You can return to this level of power subsystem firmware if you decide to remove the installed level.

The existing levels of power subsystem firmware appear on the HMC interface as shown in the highlighted row in following figure.

**Note:** The values shown in the following figure are used for example purposes only.



Target name: SYS001*12345XX

Concurrent LIC update status: Your Status

Current LIC repository location: Your Repository

| EC Number | LIC Type | Machine Type/ Model/ Serial Number | Installed Level | Activated Level | Accepted Level |
|---|---|---|---|---|---|
| 02AB123 | Power Subsystem | SYS002*12345XX | 4 | 4 | 4 |
| 01AB123 | Managed System | SYS001*12345XX | 60 | 60 | 60 |

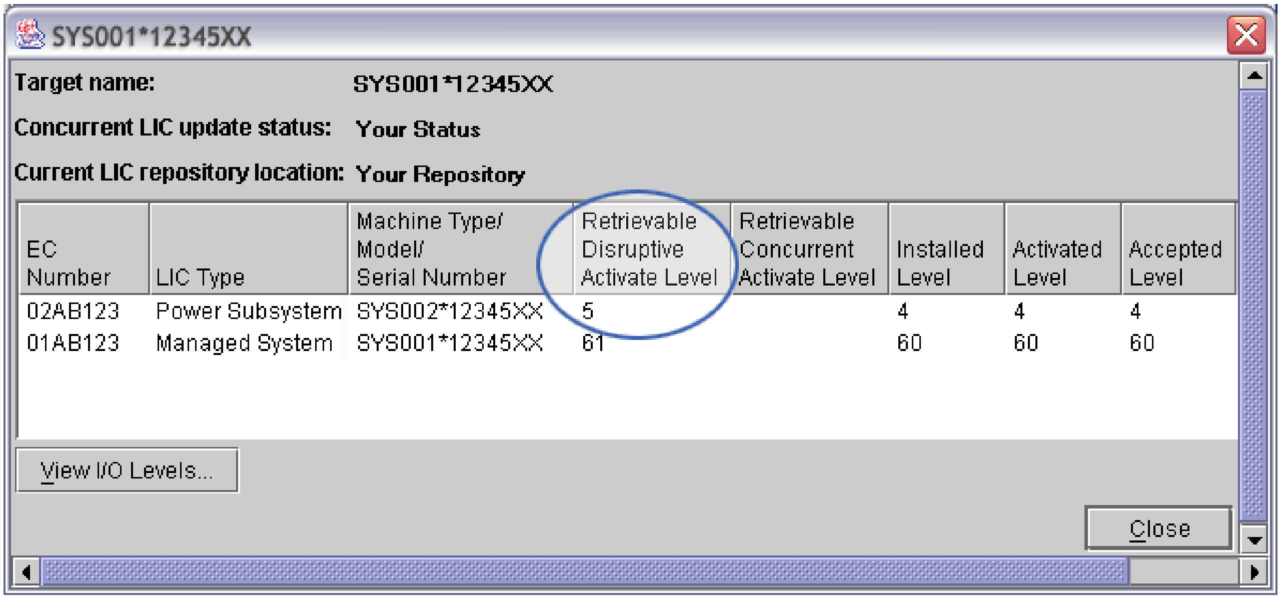
For instructions on how to view the levels of power subsystem firmware, see View existing levels of power subsystem firmware.

**Available levels of power subsystem firmware**

When the service provider issues power subsystem firmware fixes, you can view the levels of power subsystem firmware (fixes) that can be downloaded and installed from each repository location to your server.

The following figure shows the retrievable level of power subsystem firmware and other levels of power subsystem firmware. See the detailed descriptions of the retrievable level of power subsystem firmware following the figure.

**Note:** The values shown in the following figure are used for example purposes only.



SYS001*12345XX

Target name: SYS001*12345XX

Concurrent LIC update status: Your Status

Current LIC repository location: Your Repository

| EC Number | LIC Type | Machine Type/ Model/ Serial Number | Retrievable Disruptive Activate Level | Retrievable Concurrent Activate Level | Installed Level | Activated Level | Accepted Level |
|---|---|---|---|---|---|---|---|
| 02AB123 | Power Subsystem | SYS002*12345XX | 5 | | 4 | 4 | 4 |
| 01AB123 | Managed System | SYS001*12345XX | 61 | | 60 | 60 | 60 |

- **Retrievable disruptive activate level** - This is the highest level of power subsystem firmware available at the selected repository. Activation of this level of power subsystem firmware is a disruptive process. Therefore, you will be instructed to shut down all of the applications and logical partitions before initiating the installation, and the managed system will be automatically returned to its original state at the end of the process.
- **Retrievable concurrent activate level** - This is the highest level of power subsystem firmware available at the selected repository that can be retrieved, installed, and activated concurrently. Activation of this level of power subsystem firmware is a concurrent process. Therefore, it is not necessary to shut down the logical partitions or the managed system before initiating the update, and it is not necessary to power on and off the managed system to activate the fix.

**Scenarios: Power subsystem firmware fixes:** The following scenario demonstrates how you can download and install power subsystem firmware fixes to your system. Use the scenario to guide you through the process of getting fixes for your power subsystem firmware.

> **Scenario: Get power subsystem firmware fixes with an HMC**
> This scenario demonstrates how to use the HMC to download and install the power subsystem firmware fixes.

*Scenario: Get power subsystem firmware fixes with an HMC:* **Situation**

Suppose you are the system administrator for your company. You use an HMC to manage your server and you have configured several partitions on the server. Periodically, you need to download and install fixes for your power subsystem firmware.

There are several repository locations from which you can download the fixes using the HMC. For example, you can download the fixes from your service provider's Web site or support system, from optical media that you order from your service provider, or from an FTP server on which you previously placed the fixes. You can use the interface on the HMC to select any one of these repositories from which you can download and install the power subsystem firmware fixes. The Change Internal Code wizard provides a step-by-step process for you to select the appropriate repository and perform the required steps to download and install the fix.

**Objectives**

The objective of this scenario is to use the HMC to download and install the power subsystem firmware fix.

**Configuration steps**

You must complete the following tasks:
1. Ensure you have a connection to the service provider.
2. Determine the available levels of power subsystem firmware.
3. Use the Change Internal Code wizard to update your power subsystem firmware.
4. Verify that the fix installed successfully.

*Scenario details: Get power subsystem firmware fixes with an HMC:* **Step 1: Ensure you have a connection to the service provider.**

To download power subsystem firmware fixes from the service provider's system or Web site, you need to set up a connection to the service provider either through a local or remote modem or through a VPN connection. You typically set up the service connection when you first set up your server. However, the service connection is not required for initial server setup. Therefore, you need to verify that the service connection exists.

To verify the service connection, follow these steps:
1. In the navigation area, open Service Applications.
2. Select **Remote Support**.
3. Select **Customize Outbound Connectivity**.
4. Select the tab for the type of outbound connectivity you chose for your HMC (Local Modem, Internet VPN, or Pass-Through Systems). For more information about these settings, see Choosing your connection method.

   **Note:** If a connection to the service provider does not exist, you need to set up the service connection before proceeding with this scenario. For instructions on how to set up a connection to the service provider, see Scenarios: Service and support.
5. Click **Test**.
6. Verify that the test completes successfully. If the test is not successful, you need to troubleshoot your connectivity and correct the problem before proceeding with this scenario.

**Step 2: (Optional) Determine the available levels of power subsystem firmware**

This step is optional because it is not necessary to determine the available levels of power subsystem firmware before downloading and installing new fixes. The Change Internal Code wizard checks the available levels for you and by default installs the highest concurrent level of power subsystem firmware fix. If no power subsystem firmware fixes are currently available for your server, a message is displayed that indicates no fixes are available.

However, if you want to check the available levels before you download and install the fixes, you can perform this step. Then, after you get the fix, you can verify that the correct level of power subsystem firmware was installed.

If you do not want to check the available levels of power subsystem firmware, skip to Step 3.

To determine the available levels of power subsystem firmware for the managed system, follow these steps:

**Note:** The HMC interface refers to *power subsystem firmware* as *Licensed Internal Code*.
1. Expand the **Licensed Internal Code Maintenance** folder.

2. Click the **Licensed Internal Code Updates** icon.
3. In the Contents area, click **Change Internal Code**.
4. In the Target Object Selection window, click the target system, and click **OK**.
5. In the Change Internal Code window, select **View system information** and click **OK**.
6. In the Specify LIC Repository window, select the repository location from which you want to view available power subsystem firmware fixes, and click **OK**. For more information about each of the repositories, click **Help**.

   A window is displayed that shows system information for the target system, including the retrievable levels of power subsystem firmware. For details about the system information contained in the table, click **Help**.

**Step 3: Use the Change Internal Code wizard to update your power subsystem firmware.**

To use the Change Internal Code wizard to download and install your power subsystem firmware, follow these steps:

**Note:** The HMC interface refers to *power subsystem firmware* as *Licensed Internal Code*.

1. Expand the **Licensed Internal Code Maintenance** folder.
2. Click the **Licensed Internal Code Updates** icon.
3. In the Contents area, click **Change Internal Code**.
4. In the Target Object Selection window, click the target system, and click **OK**.
5. In the Change Internal Code window, select **Start Change Internal Code wizard**, and click **OK**.
6. In the Specify LIC Repository window, select the repository location from which you want to download the power subsystem firmware fixes, and click **OK**. For more information on each of the repository locations, click **Help**.
7. In the Change Internal Code Wizard welcome window, click **Next**.

   **Note:** If no fixes are available, a message is displayed that indicates no fixes are available and targets are up-to-date. In this situation, click **Cancel** to end the task.
8. In the Change Internal Code Wizard window, ensure that **Managed System and Power LIC** is selected, and click **Next**.

   **Note:** If I/O firmware fixes are available, additional windows might be displayed. Follow the instructions in these windows to install the I/O firmware fixes.
9. In the Hardware Management Console License Agreement window, read the agreement and click **Accept**.
10. In the Confirm the Action window, perform the required actions, and click **Finish**.

    If the process is disruptive, the following message is displayed on the HMC interface: `Quiesce any applications currently running on your operating systems for the systems listed below.` In this situation, you need to manually shut down all of the applications and logical partitions to prevent the system from shutting them down abnormally during the process.

    Use the normal procedures to shut down the logical partitions:

    - i5/OS logical partitions
      To shut down i5/OS logical partitions, use the Power Down System (PWRDWNSYS) command from an i5/OS command line (either in a 5250 emulator session on your HMC, or on the Operations Console). For further instructions, see Shutting down i5/OS logical partitions.
    - AIX logical partitions
      For instructions, see Shutting down AIX.
    - Linux logical partitions
      For instructions, see Shutting down Linux.

    At the end of a disruptive process, the managed system automatically returns to its original state.

**Step 4: Verify that the fix installed successfully**

To verify that the power subsystem firmware fix installed successfully, follow these steps:

**Note:** The HMC interface refers to *power subsystem firmware* as *Licensed Internal Code*.

1. Expand the **Licensed Internal Code Maintenance** folder.
2. Click the **Licensed Internal Code Updates** icon.
3. In the Contents area, click **Change Internal Code**.
4. In the Target Object Selection window, click the target system, and click **OK**. The target is the managed system for which you want to verify the power subsystem firmware level.
5. In the Change Internal Code window, select **View system information**, and click **OK**.
6. In the Specify LIC Repository window, select **None**, and click **OK**.

   A window is displayed that shows system information for the target system.
7. Verify that the installed and activated levels of power subsystem firmware match the fix that you installed.

**Manage power subsystem firmware fixes:** You can manage your power subsystem firmware fixes in several ways. Read the following topics for details.

**Note:** For instructions on how to download and install new power subsystem firmware fixes, see Scenarios: power subsystem firmware

- View existing levels of power subsystem firmware
  Find out how to view the level of power subsystem firmware that currently runs on your server.
- View available levels of power subsystem firmware
  Find out how to view the levels of power subsystem firmware that are available for you to download as fixes.
- View power subsystem firmware fix cover letter
  Find out how to view the power subsystem firmware fix cover letter.
- Get specific power subsystem firmware fix
  Find out how to download and install a specific level of power subsystem firmware rather than the highest level of power subsystem firmware.
- Install power subsystem firmware fix permanently
  Find out how to permanently install the power subsystem firmware fix.
- Remove current level of power subsystem firmware
  Find out how to remove the current level of power subsystem firmware so you can return to a previous level of power subsystem firmware.
- Upgrade to new power subsystem firmware release
  Find out how to upgrade your power subsystem firmware to a new release.

*View existing levels of power subsystem firmware:* To view the existing levels of power subsystem firmware on the managed system, follow these steps:

**Note:** The HMC interface refers to *power subsystem firmware* as *Licensed Internal Code*.

1. Expand the **Licensed Internal Code Maintenance** folder.
2. Click the **Licensed Internal Code Updates** icon.
3. In the Contents area, click **Change Internal Code**.
4. In the Target Object Selection window, click the target system, and click **OK**. The target is the managed system for which you want to check the power subsystem firmware level.
5. In the Change Internal Code window, select **View system information**, and click **OK**.
6. In the Specify LIC Repository window, select **None**, and click **OK**.

A window is displayed that shows system information for the target system. The Installed Level indicates the level of power subsystem firmware that has been installed and will be loaded into memory after the managed system is powered off and powered on. The Activated Level indicates the level of power subsystem firmware that is active and running in memory. The Accepted Level indicates the backup level of power subsystem firmware. You can return to the backup level of power subsystem firmware if you decide to remove the installed level. For details about the system information contained in the table, click **Help**.

*View available levels of power subsystem firmware:* To view the available levels of power subsystem firmware for the managed system using the HMC, follow these steps:

**Note:** The HMC interface refers to *power subsystem firmware* as *Licensed Internal Code*.

1. Expand the **Licensed Internal Code Maintenance** folder.
2. Click the **Licensed Internal Code Updates** icon.
3. In the Contents area, click **Change Internal Code**.
4. In the Target Object Selection window, click the target system, and click **OK**.
5. In the Change Internal Code window, select **View system information** and click **OK**.
6. In the Specify LIC Repository window, select the repository location from which you want to view available power subsystem firmware fixes, and click **OK**. For more information on each of the repositories, click **Help**.

   A window is displayed that shows system information for the target system, including the retrievable levels of power subsystem firmware. For details about the system information contained in the table, click **Help**.

   **Note:** If no power subsystem firmware fixes are available at the selected repository, the columns in the table will be empty.

*View power subsystem firmware fix cover letter:* Power subsystem firmware fixes can correct known problems or add new function to the code in your current power subsystem firmware release. To find out what problems the power subsystem firmware fix will correct, or to find out what new function is included in the power subsystem firmware fix, you can view the power subsystem firmware fix cover letter.

To view the power subsystem firmware fix cover letter, follow these steps:

1. Expand the **Licensed Internal Code Maintenance** folder.
2. Click the **Licensed Internal Code Updates** icon.
3. In the Contents area, click **Change Internal Code**.
4. In the Target Object Selection window, click the target system, and click **OK**.
5. In the Change Internal Code window, select **Start Change Internal Code wizard**, and click **OK**.
6. In the Specify LIC Repository window, select the repository location from which you want to view the fix cover letter, and click **OK**. For more information about each of the repositories, click **Help**.
7. In the Change Internal Code Wizard welcome window, click **Next**.

   **Note:** If no fixes are available, a message is displayed that indicates no fixes are available and targets are up-to-date. In this situation, click **Cancel** to end the task.
8. In the Change Internal Code Wizard window, ensure that **Managed System and Power LIC** is selected, and click **Advanced Options...**.

   **Note:** If I/O firmware fixes are available, an additional window might be displayed.
9. In the Managed System and Power Licensed Internal Code (LIC) Concurrency window, select the managed system, and click **View information**.

10. In the Managed System and Power Licensed Internal Code (LIC) Level Details window, select the LIC Type for which you want to view the power subsystem firmware fix cover letter, and click **View Details**. For example, you might select **Power Subsystem**.

    The power subsystem firmware fix cover letter is displayed. Read the cover letter to learn about what problems the power subsystem firmware fix will correct, or to find out what new function is included in the power subsystem firmware fix.

*Get specific power subsystem firmware fix:* You can download and install a specific level of power subsystem firmware rather than the highest (most recent) level fix.

To get a specific power subsystem firmware fix, follow these steps:

**Note:** The HMC interface refers to *power subsystem firmware* as *Licensed Internal Code*. Similarly, the HMC interface refers to *power subsystem firmware fix* as *Licensed Internal Code level*.

1. Expand the **Licensed Internal Code Maintenance** folder.
2. Click the **Licensed Internal Code Updates** icon.
3. In the Contents area, click **Change Internal Code**.
4. In the Target Object Selection window, click the target system, and click **OK**.
5. In the Change Internal Code window, select **Select advanced features**, and click **OK**.
6. In the Advanced features window, select **Install and activate (implied retrieve)**, and click **OK**.
7. In the Specify LIC Repository window, select the repository location from which you want to download and install the specific power subsystem firmware fix, and click **OK**. For more information about each of the repositories, click **Help**.
8. In the Install and Activate (Implied Retrieve) window, select **Specific levels** for LIC level type, and click **OK**.
9. In the Specify LIC Levels window, select the LIC type for which you want to choose a specific level, and click **Change Level...**. For example, you might select **Power Subsystem**.
   - In the Select LIC Level window, select the LIC level you want to install, and click **OK**. Select **None** if you do not want to update the selected LIC type.

     The Specify LIC Levels window is displayed again, showing the EC number, LIC type, Machine Type/Model/Serial Number, and LIC level that you selected in addition to other power subsystem firmware code that is available to be updated. During this process, all power subsystem firmware code with the same EC number as the LIC type you selected will be updated to the LIC level you selected.
   - In the Specify LIC Levels window, verify that the LIC levels for the power subsystem firmware code displayed in the table are correct, and click **OK**.
10. This step applies only if the process is disruptive. In the Select Installation Type window, select **Concurrent install only, with deferred disruptive activate** if you want to install the power subsystem firmware fix now and activate the power subsystem firmware fix later, or select **Disruptive install and activate** if you want to install and activate the power subsystem firmware level immediately, and click **OK**.
11. In the Hardware Management Console License Agreement window, read the agreement and click **Accept**.
12. In the Confirm the Action window, perform the required actions, and click **OK**.

    If the process is disruptive, the following message is displayed on the HMC interface: `Quiesce any applications currently running on your operating systems for the systems listed below.` In this situation, you need to manually shut down all of the applications and logical partitions to prevent the system from shutting them down abnormally.

    Use the normal procedures to shut down the logical partitions:
    - i5/OS logical partitions
      To shut down i5/OS logical partitions, use the Power Down System (PWRDWNSYS) command

from an i5/OS command line (either in a 5250 emulator session on your HMC, or on the Operations Console). For further instructions, see Shutting down i5/OS logical partitions.

- AIX logical partitions
  For instructions, see Shutting down AIX.
- Linux logical partitions
  For instructions, see Shutting down Linux.

At the end of a disruptive process, the managed system automatically returns to its original state.

*Install power subsystem firmware fix permanently:* After you download and install a power subsystem firmware fix, the fix is temporarily installed until you install it permanently. You might want to use the new level of power subsystem firmware for a period of time to verify that it works properly. When you are sure that the new level of power subsystem firmware works properly, you can permanently install the power subsystem firmware fix, so that the server is ready to install the next power subsystem firmware fix when it becomes available.

**Note:** You might recognize the process of installing the power subsystem firmware fix permanently by different terms, depending on the type of hardware or software you use. For example, if you use AIX or Linux, you might refer to this process as *committing* the fix. If you use i5/OS, you refer to this process as *applying* the fix. If you use an HMC, you might refer to this process as *accepting* the fix.

To permanently install the power subsystem firmware fix, follow these steps:

**Note:** The HMC interface refers to *power subsystem firmware* as *Licensed Internal Code*.

1. Expand the **Licensed Internal Code Maintenance** folder.
2. Click the **Licensed Internal Code Updates** icon.
3. In the Contents area, click **Change Internal Code**.
4. In the Target Object Selection window, click the target system, and click **OK**. The target is the managed system on which you want to permanently install the power subsystem firmware fix.
5. In the Change Internal Code window, select **Select advanced features** and click **OK**.
6. In the Advanced Features window, select **Accept**, and click **OK**.
7. In the Confirm the Action window, click **OK**.

*Remove current level of power subsystem firmware:* You can remove the current level of power subsystem firmware if you want to return to a previous level of power subsystem firmware.

To remove the current level of power subsystem firmware, follow these steps:

**Note:** The HMC interface refers to *power subsystem firmware* as *Licensed Internal Code*.

1. Expand the **Licensed Internal Code Maintenance** folder.
2. Click the **Licensed Internal Code Updates** icon.
3. In the Contents area, click **Change Internal Code**.
4. In the Target Object Selection window, click the target system, and click **OK**. The target is the managed system from which you want to remove the current level of power subsystem firmware.
5. In the Change Internal Code window, select **Select advanced features** and click **OK**.
6. In the Advanced Features window, select **Remove and activate**, and click **OK**.
7. In the Confirm the Action window, perform the required actions, and click **OK**.

   If the process is disruptive, the following message is displayed on the HMC interface: `Quiesce any applications currently running on your operating systems for the systems listed below.` In this situation, you need to manually shut down all of the applications and logical partitions to prevent the system from shutting them down abnormally.

Use the normal procedures to shut down the logical partitions:

- i5/OS logical partitions
  To shut down i5/OS logical partitions, use the Power Down System (PWRDWNSYS) command from an i5/OS command line (either in a 5250 emulator session on your HMC, or on the Operations Console). For further instructions, see Shutting down i5/OS logical partitions.
- AIX logical partitions
  For instructions, see Shutting down AIX.
- Linux logical partitions
  For instructions, see Shutting down Linux.

At the end of a disruptive process, the managed system automatically returns to its original state.

*Upgrade to new power subsystem firmware release:* To upgrade to a new power subsystem firmware release, follow these steps:

**Note:** The HMC interface refers to *power subsystem firmware* as *Licensed Internal Code*.

1. Obtain optical media that contains the new power subsystem firmware release from your service provider.
2. Insert optical media into the drive on the HMC.
3. Expand the **Licensed Internal Code Maintenance** folder.
4. Click the **Licensed Internal Code Updates** icon.
5. In the Contents area, click **Manufacturing Equipment Specification Upgrade**.
6. In the **Target Object Selection** window, click the target system, and click **OK**. The target is the managed system for which you want to upgrade the power subsystem firmware to a new release.
7. In the Hardware Management Console License Agreement window, read the agreement and click **Accept**.
8. In the **Manufacturing Equipment Specification Upgrade — Confirm the Action** window, perform any required actions, and click **OK**.

   The following message might be displayed on the HMC interface: `Quiesce any applications currently running on your operating systems for the systems listed below.` In this situation, you need to manually shut down all of the applications and logical partitions to prevent the system from shutting them down abnormally.

   Use the normal procedures to shut down the logical partitions:

   - i5/OS logical partitions
     To shut down i5/OS logical partitions, use the Power Down System (PWRDWNSYS) command from an i5/OS command line (either in a 5250 emulator session on your HMC, or on the Operations Console). For further instructions, see Shutting down i5/OS logical partitions.
   - AIX logical partitions
     For instructions, see Shutting down AIX.
   - Linux logical partitions
     For instructions, see Shutting down Linux.

   At the end of a disruptive process, the managed system automatically returns to its original state.

## I/O adapter and device firmware fixes

I/O adapter and device firmware is the part of the Licensed Internal Code that enables hardware, such as Ethernet PCI adapters or disk drives. As with other software, your I/O adapter and device firmware sometimes requires a fix.

Depending on your service environment and your operating systems, you can get your I/O adapter and device firmware fixes using different interfaces and methods:

- **AIX—** If you use an HMC to manage your server, you can use the HMC interface to download and install your I/O adapter and device firmware fixes. If you do not use an HMC to manage your server, you can use the functions specific to your operating system to work with I/O adapter and device firmware fixes. For instructions about how to get your I/O adapter and device firmware fixes in each of these situations, see Scenario: Get I/O adapter and device firmware fixes with an HMC (AIX) and Scenario: Get I/O adapter and device firmware fixes without an HMC.

- **i5/OS —** I/O adapter and device firmware PTFs for i5/OS partitions are ordered, packaged, delivered, and installed as part of the Licensed Internal Code using the same processes that apply to i5/OS PTFs. Regardless of whether you use an HMC to manage your server, you use the normal i5/OS PTF installation functions on each logical partition to download and install the I/O adapter and device firmware fixes firmware fixes. For instructions on how to install fixes for i5/OS, see Order fixes.

Use the following information to learn more about I/O adapter and device firmware fixes:

- Scenarios: I/O adapter and device firmware fixes
  Use these scenarios to learn how to download and install I/O adapter and device firmware fixes, either through the HMC or through the operating system.

**Scenarios: I/O adapter and device firmware fixes:** These scenarios demonstrate several ways you can download and install I/O adapter and device firmware fixes to your system. Use the scenarios to guide you through the process of getting fixes for your I/O adapter and device firmware.

> **Scenario: Get I/O adapter and device firmware fixes with an HMC (AIX)**
> This scenario demonstrates how to use the HMC to download and install the I/O adapter and device firmware fixes for logical partitions running AIX.
>
> **Scenario: Get I/O adapter and device firmware fixes without an HMC**
> This scenario demonstrates how to download and install I/O adapter and device firmware fixes through your operating system when you do not use an HMC to manage your system.

*Scenario: Get I/O adapter and device firmware fixes with an HMC (AIX):* **Situation**

Suppose you are the system administrator for your company. You use an HMC to manage your server and you have configured several partitions on the server. Periodically, you need to download and install fixes for your I/O adapter and device firmware.

You know that you can use the HMC to download and install I/O adapter and device firmware for your AIX logical partitions. There are several repository locations from which you can download the fixes using the HMC. You can download the fixes from your service provider's Web site, from optical media that you order from your service provider, or from an FTP server on which you previously placed the fixes. You can use the interface on the HMC to select any one of these repositories from which you can download and install the I/O adapter and device firmware fixes. The Change Internal Code wizard provides a step-by-step process for you to select the appropriate repository and perform the required steps to download and install the fix.

**Objectives**

The objective of this scenario is to use the HMC to download and install the I/O adapter and device firmware fix.

**Configuration steps**

You must complete the following tasks:

1. Ensure you have a connection to the service provider.
2. Use the Change Internal Code wizard to update your I/O adapter and device firmware.
3. Verify that the fix installed successfully.

*Scenario details: Get I/O adapter and device firmware fixes with an HMC (AIX ):* **Step 1: Ensure you have a connection to the service provider.**

To download I/O adapter and device firmware fixes from the service provider's system or Web site, you need to set up a connection to the service provider either through a local or remote modem or through a VPN connection. You typically set up the service connection when you first set up your server. However, the service connection is not required for initial server setup. Therefore, you need to verify that the service connection exists.

To verify the service connection, follow these steps:

1. In the navigation area, open Service Applications.
2. Select **Remote Support**.
3. Select **Customize Outbound Connectivity**.
4. Select the tab for the type of outbound connectivity you chose for your HMC (Local Modem, Internet VPN, or Pass-Through Systems). For more information about these settings, see Choosing your connection method.

   **Note:** If a connection to the service provider does not exist, you need to set up the service connection before proceeding with this scenario. For instructions on how to set up a connection to the service provider, see Scenarios: Service and support.
5. Click **Test**.
6. Verify that the test completes successfully. If the test is not successful, you need to troubleshoot your connectivity and correct the problem before proceeding with this scenario.

**Step 2: Use the Change Internal Code wizard to update your I/O adapter and device firmware.**

To use the Change Internal Code wizard to download and install your I/O adapter and device firmware, follow these steps:

**Note:** The HMC interface refers to *I/O adapter and device firmware* as *Licensed Internal Code*.

1. Expand the **Licensed Internal Code Maintenance** folder.
2. Click the **Licensed Internal Code Updates** icon.
3. In the Contents area, click **Change Internal Code**.
4. In the Target Object Selection window, click the target system, and click **OK**.
5. In the Change Internal Code window, select **Start Change Internal Code wizard**, and click **OK**.
6. In the Specify LIC Repository window, select the repository location from which you want to download the I/O adapter and device firmware fixes, and click **OK**. You can download and install I/O adapter and device firmware fixes from any of the following repository locations:
   - **IBM service Web site**
   - **DVD drive**
   - **FTP site**

   For more information on each of the repository locations, click **Help**.
7. In the Change Internal Code Wizard welcome window, click **Next**.

   **Note:** If no fixes are available, a message is displayed that indicates no fixes are available and targets are up-to-date. In this situation, click **Cancel** to end the task.

   One of two windows is displayed, depending on the type of firmware fixes that are currently available to download and install from the selected repository:
   - If server firmware fixes or power subsystem firmware fixes are available, the Change Internal Code Wizard window is displayed with **Managed System and Power LIC** preselected.

     Choose one of the following options:

- If you want to download and install the server firmware fixes or power subsystem fixes now, click **Next**, and follow the instructions in the subsequent windows to install the server firmware fixes or power subsystem fixes.
- If you do not want to install the server firmware fixes or power subsystem fixes now, deselect **Managed System and Power LIC**, and click **Next**.

- If I/O adapter and device firmware fixes are available, the Change Internal Code Wizard window is displayed either with **I/O LIC** preselected or not selected.

8. In the Change Internal Code Wizard window, ensure that **I/O LIC** is selected, and click **Advanced Options**.
9. In the Licensed Internal Code Survey Results window, select the adapters or devices for which you want to download and install firmware fixes, and click **OK**.

   **Note:** The system preselects the adapters or devices with the following characteristics:
   - The HMC can manage the adapters or devices.
   - Firmware fixes are currently available.
   - The adapters or devices do not need to be taken offline when you install the firmware fixes.

   You can change the preselected adapters or devices in the table to identify the I/O adapter and device firmware fixes that you want to install.

   Use the information in the column entitled `Effect` to determine whether the adapters or devices require you to shut down the adapter or device when you install the I/O adapter or device firmware fixes.

   Use the information in the column entitled `Suggested Action` to determine whether the HMC can manage the I/O adapters or devices listed in the table. If the `Suggested Action` column indicates `Cannot Manage`, you need to download and install the I/O adapter and device firmware fix through the operating system. For more information, see Scenario: Get I/O adapter and device firmware fixes without an HMC. For more information about the table, click **Help**.
10. In the Change Internal Code wizard window, click **Next**.
11. In the Hardware Management Console License Agreement window, read the agreement and click **Accept**.
12. In the Confirm the Action window, perform the required actions, and click **Finish**.

**Step 3: Verify that the fix installed successfully**

To verify that the I/O adapter and device firmware fix installed successfully, follow these steps:

**Note:** The HMC interface refers to *I/O adapter and device firmware* as *Licensed Internal Code*.

1. Expand the **Licensed Internal Code Maintenance** folder.
2. Click the **Licensed Internal Code Updates** icon.
3. In the Contents area, click **Change Internal Code**.
4. In the Target Object Selection window, click the target system, and click **OK**. The target is the managed system for which you want to verify the I/O adapter and device firmware level.
5. In the Change Internal Code window, select **View system information**, and click **OK**.
6. In the Specify LIC Repository window, select the repository location that you selected in Step 2, and click **OK**.

   A window is displayed that shows system information for the target system.
7. In the window, click **View I/O Levels**.
8. In the Licensed Internal Code Survey Results window, verify that the firmware level indicated in the column entitled `Current Level` matches the fix that you installed.

### *Scenario: Get I/O adapter and device firmware fixes without an HMC:* Situation

Suppose you are the system administrator for your company. Your server is in its manufacturing default configuration, and you do not use an HMC to manage your server. Periodically, you need to download and install fixes for your I/O adapter and device firmware. Because you do not use an HMC to manage your server, you must get your fixes through your operating system. In this situation, you can get I/O adapter and device firmware fixes through the operating system regardless of whether your operating system is AIX, Linux, or i5/OS.

#### Objectives

The objective of this scenario is to download and install the I/O adapter and device firmware fix through your operating system.

#### Configuration steps

You must complete the following tasks:
1. Ensure you have a connection to the service provider.
2. Download and install the I/O adapter and device firmware fixes.

### *Scenario details: Get I/O adapter and device firmware fixes without an HMC:* Step 1: Ensure you have a connection to the service provider.

To download I/O adapter and device firmware fixes from the service provider, you need to set up a connection to the service provider, either through a local or remote modem or through a VPN connection. You typically set up the service connection when you first set up your server. However, the service connection is not required for initial server setup. Therefore, you need to verify that the service connection exists.

If a connection to the service provider does not exist, you need to set up the service connection before proceeding with this scenario. For instructions on how to set up a connection to the service provider, see Scenarios: Service and support.

#### Step 2: Download and install the I/O adapter and device firmware fixes

The method you use to download and install the I/O adapter and device firmware fixes depends on your operating system:

- **i5/OS**
  I/O adapter and device firmware PTFs for i5/OS partitions are ordered, packaged, delivered, and installed as part of the Licensed Internal Code using the same processes that apply to i5/OS PTFs. Use the i5/OS PTF installation functions on each logical partition to download and install the I/O adapter and device firmware fixes. For instructions on how to install i5/OS fixes, see Order fixes.
- **AIX or Linux**
  To download and install the I/O adapter and device firmware fix, follow these steps:

  **Note:** If you are accessing this information from the Download microcode Web site, skip to Step 3 to start this task.

  1. Go to Fix Central .
     a. In the **Server** list, click **pSeries family**.
     b. In the **Product or fix type** list, click **Hardware microcode and firmware**.
     c. Click **Continue**.
  2. From the Microcode updates for pSeries® servers and RS/6000® Web site, click **Microcode downloads**.

3. From the Download microcode Web site, click **Adapter**, **Other**, or **DASD**, depending on the type of adapter or device for which you want to get a fix, and follow these steps:
   a. In the `Model` column, find the adapter or device for which you want to download and install a fix.
   b. In the associated `Download` column, click **Description**, and read the instructions for downloading and installing the I/O adapter and device firmware fix to your server.

### Operating system fixes

To keep your partitions running smoothly, it is important that you install fixes for your operating system code when fixes are available.

You can access fixes for your operating systems using Fix Central.

From the Web site, follow these steps:

1. In the **Server** list, click the appropriate family. For example, **iSeries family** or **pSeries family**.
2. In the **Product or fix type** list, click the operating system for which you want to get a fix.
3. Depending on your selections for **Server** and **Product or fix type**, you might see additional lists from which you can select specific options.
4. Click **Continue**.

For more information about fixes for the operating systems, see the following Web sites:

- **AIX:** Go to Support for pSeries products.
- **i5/OS:** Go to Maintain and manage i5/OS and related software.
- **Linux:** Go to Support for pSeries products.

## Enabling remote support

Remote support enables you to securely give your service provider access to your HMC or server to enable problem analysis and determination. The following topics describe remote support in more detail:

**Remote support methods**
Use this information to learn about the remote support methods that are available to you.

**Enabling remote support on the HMC**
Use this information to learn how to allow your service provider to access your server or HMC.

**Enabling remote support without an HMC**
Use this information to learn how to enable remote support when you do not have an HMC.

### Remote support methods

If you are using your server with an HMC, you can use the following communication methods to enable this connection:

- **Virtual private networking (VPN)—** A virtual private network (VPN) allows your company to securely extend its private intranet over the existing framework of a public network, such as the Internet. With VPN, your company can control network traffic while providing security features such as authentication and data privacy. This protocol is very efficient over high-speed Internet connections.

  VPN also supports Layer 2 Tunneling Protocol (L2TP) solutions. L2TP connections, which are also called *virtual lines*, provide cost-effective access for remote users by allowing a corporate network server to manage the IP addresses assigned to its remote users. Further, L2TP connections provide secure access to your system or network when you protect them with IP Security.

- **Point-to-Point Protocol (PPP)**— This method is a standard for transmitting data over telephone lines. It is the most widely used connection protocol among Internet service providers. PPP allows individual computers to access networks, which in turn provide access to the Internet.

For examples and configuration details about both of these methods of connectivity, see Scenarios: i5/OS.

## Enabling remote support on the HMC

To enable remote support personnel to access your HMC or server, follow these steps:

1. In the navigation area, open Service Applications.
2. Select **Remote Support**.
3. Select **Customize Inbound Connectivity**.

In most cases, you can enable remote support only when you are present to work with your service provider. This is called an *attended session*. However, you can also set your HMC's modem to answer incoming service calls or use a combination of call-in and call-back settings for *unattended sessions*.

## Enabling remote support without an HMC

If your server is in its manufacturing default configuration, you can still enable support personnel to do problem determination. For more information, see the following:

- **AIX and Linux** – If you have AIX or Linux installed on your server, you can enable your service provider to call in to your server through the service processor. For more information about configuring your service processor for call-in and call-out, see Setting up the service processor to connect to the service provider.
- **i5/OS** – If you have i5/OS installed on your server, you use the same methods for remote support that you used on earlier server models. For more information, see the Remote support topic collection.

# Related information for customer service and support

Listed below are sources of information that relate to the Customer service and support topic collection.

**Web sites**

- Online Publications
  This Web site enables you to search for the appropriate simplified activation user's guide for Electronic Service Agent running on i5/OS.

- Fix Central
  This Web site enables you to search for the fixes you need for server firmware, HMC machine code, and operating systems.

- IBM eServer Prerequisite
  This Web site enables you to determine the minimum levels of operating system fixes and server firmware fixes that are required for specific hardware.

- iSeries Information Center
  The iSeries Information Center is a source for technical information about the iSeries server. The information center is your starting point for all iSeries technical information.

- Electronic Service Agent
  This Web site enables you to search for the appropriate user's guide for Electronic Service Agent running on AIX and Linux.

- IBM eServer Support — Linux on Power
  This Web site enables you to download service tools.

**Other information**

- Managing your server

- Troubleshooting

### 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
e(logo)server
eServer
i5/OS
IBM
iSeries
pSeries
RS/6000

Intel, Intel Inside (logos), MMX and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

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.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

## Communications statements

The following Class A statements apply to these models:

5790<br>
5791
5794
7311-D10
7311-D11
7311-D20
9111-520 (rack-mounted version)
9113-550
9117-570
9119-590
9119-595
9124-720
9405-520
9406-520
9406-550
9406-570
9406-595
9411-100

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**

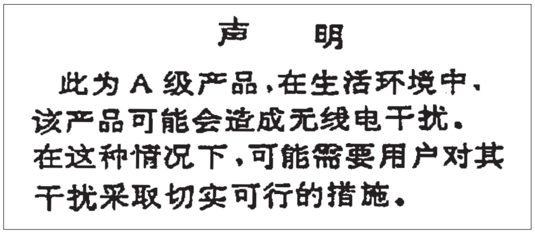
この装置は、クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。　ＶＣＣＩ－Ａ

The following is a summary of the 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*):



声　明

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

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

**Electromagnetic Interference (EMI) Statement - Taiwan**

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

The following is a summary of the 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**

Dieses Gerät ist berechtigt in Übereinstimmung mit Dem deutschen EMVG vom 9.Nov.92 das EG–Konformitätszeichen zu führen.

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:

Geräte dürfen an Orten, für die sie nicht ausreichend entstört sind, nur mit besonderer Genehmigung des Bundesministers für Post und Telekommunikation oder des Bundesamtes für Post und Telekommunikation betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Störungen zu erwarten sind.

(Auszug aus dem EMVG vom 9.Nov.92, Para.3, Abs.4)

Hinweis

Dieses Genehmigungsverfahren ist von der Deutschen Bundespost noch nicht veröffentlicht worden.

The following Statement applies to this IBM product. The statement for other IBM products intended for use with this product will appear in their accompanying manuals.

## Federal Communications Commission (FCC) statement

**Note:** This equipment has been tested and found to comply with the limits for a class 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 Réglement 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.

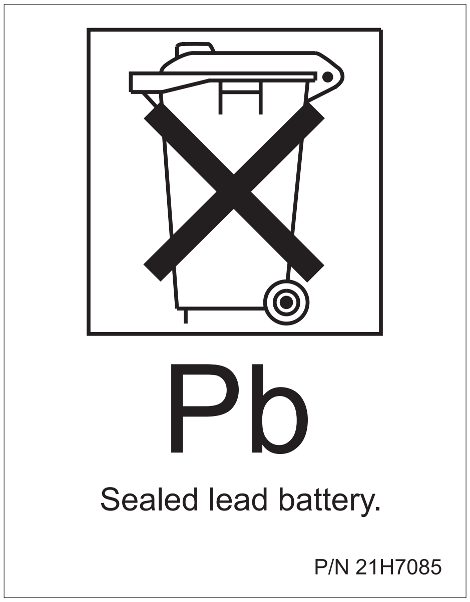
IBM encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. IBM offers a variety of programs and services to assist equipment owners in recycling their IT products. Information on product recycling offerings can be found on IBM's 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.

Printed in USA