



System i and System p
Customer service, support, and troubleshooting





System i and System p

Customer service, support, and troubleshooting

Note

Before using this information and the product it supports, read the information in “Notices” on page 453 and the *IBM Systems Safety Information* manual, G229-9054.

Twelfth Edition (September 2007)

© Copyright International Business Machines Corporation 2004, 2007.

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

Contents

Safety and environmental notices	xi
---	-----------

About this topic	xv
-----------------------------------	-----------

Customer service, support, and troubleshooting	1
---	----------

What's new for Customer service, support, and troubleshooting	1
PDF file for Customer service, support, and troubleshooting	1
Overview of service and support	2
Elements of your service environment	3
Connectivity	3
Choosing your connection method	4
Selecting the order for connectivity	5
Service information	5
Electronic problem reporting	6
Updates overview	7
Remote support	7
Using the service applications	8
Electronic Service Agent	9
Service Focal Point	10
Remote Support Facility	11
Map of service applications and functions	11
Scenarios: Service and support	13
Scenarios: AIX	13
Scenario: Multiple AIX logical partitions with an HMC	13
Scenario: Multiple servers running AIX without an HMC	16
Scenarios: IBM i5/OS	18
Scenario: Multiple IBM i5/OS logical partitions using a direct Internet connection on an i5/OS logical partition	18
Scenario: Multiple IBM i5/OS logical partitions using the HMC's modem	20
Scenario: Multiple IBM i5/OS logical partitions using the modem on an i5/OS logical partition	22
Scenario: Multiple IBM i5/OS logical partitions using the HMC modem and the modem on an i5/OS logical partition	25
Scenario: IBM i5/OS without an HMC using direct Internet	27
Scenario: Linux without an HMC	29
Setting up your service environment	31
Setting up your server to connect to service and support	31
Setting up a 7037-A50 or a 7047-185 system to connect to service and support	31
Task 1. Before you begin	31
Task 2. Decide on your connectivity method	32
Task 3. Prerequisites	32
Task 4. Ensure that your physical networking is set up correctly.	32
Task 5. Obtain or verify an IBM ID	32
Task 6. Install the operating system on your server	33
Task 7. Configure your TCP/IP network.	33
Task 8. Activate TCP/IP on your server or logical partitions	33
Task 9. Obtain and configure Electronic Service Agent for AIX or Linux	33
Task 10. Use the Service Agent (SA) Basic User Interface	35
Task 11. Register the ID with Electronic Service Agent for AIX or Linux	36
Task 12. Test the connection to service and support	36
Task 13. View the server information that was reported.	37
Setting up a clustered environment to connect to service and support	37
Task 1. Before you begin	37
Task 2. Decide on your connectivity method	37
Task 3. Prerequisites	38
Task 4. Ensure that your physical networking is set up correctly.	39

Task 5. Obtain or verify an IBM ID	41
Task 6. Verify the HMC service settings using the Guided Setup wizard	41
Task 7. Set up and configure your logical partitions	43
Task 8. Install the operating systems on your server or logical partitions	43
Task 9. Configure your TCP/IP network.	43
Task 10. Activate TCP/IP on your server or logical partitions.	43
Task 11. Obtain and configure Electronic Service Agent for AIX or Linux	43
Task 12. Use the Service Agent (SA) Basic User Interface	45
Task 13. Register the ID with Electronic Service Agent for AIX or Linux	46
Task 14. Configure the service processor.	46
Task 15. Test the connection to service and support	47
Task 16. View the server information that was reported.	48
Setting up AIX or Linux to use an HMC to connect to service and support	48
Task 1. Before you begin	48
Task 2. Decide on your connectivity method	48
Task 3. Prerequisites	49
Task 4. Ensure that your physical networking is set up correctly.	49
Task 5. Obtain or verify an IBM ID	51
Task 6. Verify the HMC service settings	52
Task 7. Set up and configure your logical partitions	53
Task 8. Install the operating systems on your server or logical partitions	54
Task 9. Configure your TCP/IP network.	54
Task 10. Activate TCP/IP on your server or logical partitions.	54
Task 11. Obtain and configure Electronic Service Agent for AIX or Linux	54
Task 12. Use the Service Agent (SA) Basic User Interface	56
Task 13. Register the ID with Electronic Service Agent for AIX or Linux	57
Task 14. Configure the service processor.	57
Task 15. Test the connection to service and support	58
Task 16. View the server information that was reported.	59
Setting up AIX or Linux to connect to service and support without an HMC	59
Task 1. Before you begin	59
Task 2. Decide on your connectivity method	59
Task 3. Prerequisites	60
Task 4. Ensure that your physical network is set up correctly.	60
Task 5. Obtain or verify an ID	60
Task 6. Install the operating system on your server	61
Task 7. Configure your TCP/IP network.	61
Task 8. Activate TCP/IP on your server	61
Task 9. Obtain and configure Electronic Service Agent for AIX or Linux	61
Task 10. Use the Service Agent (SA) Basic User Interface	64
Task 11. Register the ID with Electronic Service Agent for AIX or Linux	64
Task 12. Configure the service processor.	64
Task 13. Test the connection to service and support	65
Task 14. View the server information that was reported.	66
Setting up IBM i5/OS to connect to service and support with an HMC	66
Task 1. Before you begin	66
Task 2. Decide on your connectivity method	67
Task 3. Prerequisites	67
Task 4. Ensure that your physical networking is set up correctly.	68
Task 5. Obtain or verify an IBM ID	69
Task 6. Verify the HMC service settings	69
Task 7. Set up and configure your logical partitions	71
Task 8. Install the operating systems on your server or logical partitions	71
Task 9. Configure your TCP/IP network.	71
Task 10. Activate TCP/IP on your server or logical partitions.	71
Task 11. Configure Electronic Service Agent for i5/OS	71
Task 12. Register the IBM ID for i5/OS	76
Task 13. Test the connection to service and support	76
Task 14. View the server information that was reported to IBM	77
Setting up IBM i5/OS to connect to service and support without an HMC	77
Task 1. Before you begin	77

Task 2. Decide on your connectivity method	77
Task 3. Prerequisites	78
Task 4. Ensure that your physical networking is set up correctly.	78
Task 5. Obtain or verify an IBM ID	79
Task 6. Install the operating systems on your server	79
Task 7. Configure your TCP/IP network.	79
Task 8. Activate TCP/IP on your server or logical partitions	79
Task 9. Configure Electronic Service Agent for i5/OS	79
Task 10. Register the IBM ID for i5/OS	83
Task 11. Test the connection to service and support	83
Task 12. View the server information that was reported to IBM	83
Setting up AIX, IBM i5/OS, Linux, and the HMC to connect to service and support	84
Task 1. Before you begin	84
Task 2. Decide on your connectivity method	84
Task 3. Prerequisites	85
Task 4. Ensure that your physical networking is set up correctly.	86
Task 5. Obtain or verify an IBM ID	88
Task 6. Verify the HMC service settings using the Guided Setup wizard	89
Task 7. Set up and configure your logical partitions	90
Task 8. Install the operating systems on your server or logical partitions	90
Task 9. Configure your TCP/IP network.	91
Task 10. Activate TCP/IP on your server or logical partitions.	91
Task 11. Obtain and configure Electronic Service Agent for AIX or Linux	91
Task 12. Configure Electronic Service Agent for i5/OS	95
Task 13. Test the connection to service and support.	100
Task 14. View the server information that was reported	101
Ensuring security when using Electronic Service Agent	101
Transmission security.	102
Connection options	102
Privacy of client information	102
Enable remote support	102
Remote support methods	102
Enabling remote support on the HMC	103
Enabling remote support without an HMC	103
Enabling remote support without an HMC when you have AIX or Linux	103
Enabling remote support without an HMC when you have i5/OS.	103
Supporting information for setting up your service environment	104
Requirements needed by service personnel	104
Manually set up the HMC to connect to service and support	104
Supporting information for connecting the HMC to service and support.	105
Networking for your service environment.	105
Specifying the connection type from the HMC	107
Specifying your company's contact and account information	108
Configuring Electronic Service Agent on your HMC	108
Specifying options for connection monitoring.	112
Using IBM i5/OS applications and interfaces to set up connections to service and support	112
Using the Universal Connection wizard to connect IBM i5/OS to service and support	112
Using the Extreme Support wizard to connect IBM i5/OS to service and support.	113
Using IBM Performance Management for eServer iSeries	114
IP Packet Filter Firewall	114
Updates	116
Concepts for obtaining updates through the HMC	116
Levels of firmware on the HMC	117
Existing levels of server firmware and power subsystem firmware.	117
Available levels of server firmware and power subsystem firmware	118
Understanding concurrent firmware maintenance using the HMC.	119
Applying firmware to multiple managed systems using an HMC	120
DVD repository limitations.	120
Considerations for updating firmware on a 575 system	120
Temporary and permanent side of the service processor when using an HMC.	120
Obtaining updates.	121

Obtaining HMC machine code updates and upgrades	121
Obtaining machine code updates for the HMC with an Internet connection	121
Obtaining machine code updates for the HMC using CD or an FTP server	124
Updating the code on multiple HMCs using the remote command line	126
Upgrading the machine code on an HMC	127
Upgrading the machine code on an HMC from Version 6 to Version 7	132
Obtaining firmware updates	135
Obtaining server firmware updates for a 7037-A50 or 7047-185 system	135
Obtaining updates for the Virtual I/O Server.	140
Obtaining firmware updates through an HMC with an Internet connection.	141
Obtaining firmware updates through an HMC using a CD, FTP server, or hard drive	151
Obtaining server firmware updates through AIX or Linux without an HMC	160
Obtaining server firmware updates through IBM i5/OS	166
Obtaining a specific firmware update with an HMC	169
Installing a firmware update permanently.	170
Upgrading to a new firmware release through the HMC	172
Obtaining I/O adapter and device firmware updates	173
Obtaining I/O adapter and device firmware updates through an HMC with an Internet connection (AIX only)	173
Obtaining I/O adapter and device firmware updates through an HMC using CD or an FTP server (AIX only)	176
Obtaining I/O adapter and device firmware updates for a system that is not managed by an HMC and is running AIX	179
Obtaining I/O adapter and device firmware updates through IBM i5/OS	179
Obtaining operating system updates.	180
Obtaining operating system updates for AIX or Linux.	180
Obtaining operating system updates for i5/OS	180
Obtaining updates for the Virtual I/O Server.	180
Updating the Virtual I/O Server's firmware and device microcode through the Integrated Virtualization Manager with an Internet connection	181
Updating the Virtual I/O Server's firmware and device microcode through the Integrated Virtualization Manager without an Internet connection	182
Updating the Virtual I/O Server's firmware using the command line interface	184
Updating the firmware of the devices that the Virtual I/O Server manages.	184
Obtaining updates for a clustered environment	184
Managing updates.	184
Ensuring you have a connection to service and support	185
Determining your HMC machine code version and release	185
Viewing existing firmware levels	186
Using the HMC to view the existing firmware levels	186
Using the ASMI to view the existing level of server firmware	186
Using the AIX or Linux command line to view the existing firmware level	186
Using IBM i5/OS to view the installed server firmware PTFs	189
Viewing available firmware levels	190
Viewing available firmware levels with an HMC (with an Internet connection)	190
Viewing available firmware levels for AIX and Linux	191
Viewing available firmware levels for IBM i5/OS	191
Determining if your server firmware level and HMC machine code level are compatible	192
Step 1. Review your HMC machine code version and release	192
Step 2. View existing firmware levels with an HMC	192
Step 3. Update HMC machine code or server firmware	193
Viewing the firmware history or cover letter	194
Viewing the firmware cover letter with an HMC	194
Viewing the firmware history for AIX or Linux	194
Viewing the firmware cover letter for IBM i5/OS	195
Downloading an update to an FTP server	195
Removing the current firmware level	195
Using an HMC to remove the current firmware level	196
Using AIX commands and tools to remove the current server firmware level	196
Using the Linux command line to remove the current server firmware level	197
Using IBM i5/OS to remove the current server firmware level	198

Applying an earlier level of server firmware after exchanging the service processor in a model 570 or 9116-561	198
Using an HMC to apply an earlier level of server firmware after exchanging the service processor in a model 570 or 9116-561	198
Using AIX or Linux commands to apply an earlier level of server firmware after exchanging the service processor in a model 570 or 9116-561	200
Using i5/OS commands to apply an earlier level of server firmware after exchanging the service processor in a model 570 or 9116-561	200
Troubleshooting firmware updates	200
HMC system information panel shows all zeros	200
Message regarding a server that was previously managed by an HMC	201
Obtaining server firmware updates through AIX or Linux when you are unable to start the operating system or server	202
Step 1. Determine the existing level of firmware.	202
Step 2. Obtain the Microcode Update Files & Discovery Tool CD	203
Step 3. Apply the server firmware update	203
Step 4. Verify that the update installed correctly.	203
Additional information about obtaining updates.	204
Using the AIX diagnostics to install the server firmware update through AIX	204
Using the System Management Interface Tool to mount the update CD for AIX	206
Obtaining service and productivity tools for Linux	207
Working with the temporary and permanent side of the service processor	208
Using the HMC to work with the temporary and permanent side of the service processor.	208
Using AIX or Linux commands to work with the temporary and permanent side of the service processor	209
Using the IBM i5/OS tools to work with the temporary and permanent side of the service processor	210
Using the control panel to work with the temporary and permanent side of the service processor	210
Switching to the other side of the service processor using ASMI or the control panel	210
Getting started with troubleshooting	212
Managing problems	212
How you manage problems	212
How your system manages problems	213
Detecting problems	214
Attention light overview	214
Messages overview	217
Reference codes overview	218
Beginning problem analysis	219
AIX problem analysis.	221
IBM i5/OS problem analysis	224
Symptom and recovery actions	227
Recovering from a system power problem.	228
Recovering when the remote control panel interface of Operations Console is not working correctly	228
Recovering from IPL or system failures.	229
Recovering from a workstation failure	229
Recovering from a tape or CD drive problem.	230
Recovering from a communications problem	230
Recovering from system hang or loop condition.	231
Recovering from an intermittent problem	231
Recovering when the console does not show a sign-on display or a menu with a command line	231
Linux problem analysis	232
HMC problem analysis	235
Entry point for HMC problem determination.	236
Beginning HMC problem determination	237
Step 1. HMC problem determination	237
Testing the HMC	238
Testing for a power problem	238
Performing diagnostic procedures	238
Performing system unit testing using PC-Doctor.	239
Testing the modem connection to the managed system	239
Testing the HMC's modem connection	240
Testing the HMC's Ethernet adapter.	242
Testing the HMC's disk drive	242

Testing the HMC's DVD-RAM	243
Testing the HMC's diskette drive	245
Testing the HMC's display	246
Maintaining the HMC	246
Managed system operation	246
HMC system diagnostics	247
Powering on and off the HMC	247
Power off the HMC	247
Power-on self-test	247
Specifications and system unit locations	248
HMC external AC power cable	248
HMC diagnostics overview	248
Removing and replacing parts on the HMC	253
Analyzing HMC machine code problems	254
Starting an xterm shell	254
Powering on managed systems after a power outage when your HMC is configured as a DHCP server	255
Troubleshooting the keyboard, video, and mouse (KVM) switch for the 1x8 and 2x8 console manager	256
Troubleshooting monitor problems when connected to a KVM switch for the 1x8 and 2x8 console manager	257
Troubleshooting keyboard problems when connected to a KVM switch for the 1x8 or 2x8 console manager	258
Troubleshooting user port problems for the (KVM) switch on a 1x8 or 2x8 console manager	259
Troubleshooting a power problem for the KVM switch on the 1x8 or 2x8 console manager	259
Collecting reference codes and system information	260
Using the HMC to collect reference codes and system information	260
Using the Integrated Virtualization Manager to collect reference codes and system information	261
Using the control panel to collect reference codes and system information	261
Using AIX tools to collect reference codes and system information	262
Using i5/OS tools to collect reference codes and system information	263
Using Linux tools to collect reference codes and system information	263
Reference codes list for customers	263
HMC error codes	271
0xxxxx connection error codes	271
ESA0xxxx Electronic Service Agent error codes	275
HSCExxxx console events error codes	277
HSCFxxxx Licensed Internal Code error codes	277
HSCIxxxx Inventory Scout Services error codes	282
HSCLxxxx error codes	285
HSCL00xx Profile data error codes	286
HSCL01xx managed system error codes	293
HSCL02xx error codes	294
HSCL03xx managed system resource error codes	301
HSCL04xx logical partition error codes	304
HSCL05xx logical partition error codes	305
HSCL06xx error codes	310
HSCL07xx error codes	317
HSCL09xx system profile error codes	320
HSCL0Bxx attention light messages	323
HSCL0Dxx operating system reset error codes	324
HSCL0Fxx error codes	324
HSCL11xx backup and restore error codes	326
HSCL13xx utility class error codes	329
HSCL14xx error codes	330
HSCL15xx CIMOM error codes	335
HSCL17xx HMC console error codes	339
HSCL19xx WEBSM/AUIML error codes	341
HSCL24xx	348
HSCL25xx user management error codes	349
HSCL29xx user management error codes	350
HSCL3xxx error codes	359
HSCL70xx error codes	369
HSCL80xx error codes	370
HSCL90xx error codes	371

HSCLAxxx error codes	383
HSCPxxxx platform management error codes.	384
HSCSxxxx Service Focal Point error codes	392
Virtual terminal errors (Comm) error codes	404
Service request numbers (SRNs)	405
Supporting diagnostics	405
Running the online and eServer stand-alone diagnostics	405
Running the online diagnostics	405
Running the online diagnostics in service mode	406
Running the online diagnostics in maintenance mode	407
Running the online diagnostics in concurrent mode	407
Running the eServer stand-alone diagnostics from CD-ROM.	408
Running the eServer stand-alone diagnostics from CD on a server with an HMC attached.	408
Running the eServer stand-alone diagnostics from CD on a server without an HMC attached	410
Running the eServer stand-alone diagnostics from a Network Installation Management server	412
Performing a slow boot	414
Using the HMC to perform a slow boot	415
Using the control panel to perform a slow boot	415
Using the ASMI menus to perform a slow boot	416
Performing dumps	416
Performing a system dump.	417
Using the HMC to perform a system dump	417
Using the control panel to perform a system dump.	417
Using the ASMI to perform a system dump	418
Performing a service processor dump	418
Using the HMC to perform a service processor dump	418
Using the control panel to perform a service processor dump	418
Using the ASMI to perform a service processor dump	419
Performing an IBM i5/OS main storage dump	419
Using the HMC to perform an IBM i5/OS main storage dump	419
Using the control panel to perform an IBM i5/OS main storage dump	420
Virtual I/O Server dumps	420
Managing dumps	420
Copying a dump	420
Reporting a dump.	423
Deleting a dump	425
Determining the primary or alternate console	427
Primary console workstation requirements	427
Find the primary console when the system is operational.	427
Find the primary console when the system power is off	428
Correcting the managed system operating state	428
Correcting a <i>No connection</i> state for a managed system	428
Correcting an <i>Incomplete</i> state for a managed system	429
Correcting a <i>Recovery</i> state for a managed system	430
Correcting an <i>Error</i> state for a managed system	430
Correcting a <i>Failed Authentication</i> state for a managed system	430
Correcting a connection problem between the HMC and a managed system	431
Resetting the service processor	432
Resetting the managed system connection from the HMC	432
Checking for a duplicate IP address	432
Resetting a 4758 cryptographic battery that has a low battery condition using i5/OS commands	433
Step 1. Ensure you have the correct firmware level on the cryptographic coprocessor	433
Step 2. Verify that the hex 030B access control point is enabled	433
Step 3. Create and run an ILE CL program	434
Viewing messages	434
Viewing AIX messages	434
Viewing HMC messages.	435
Viewing IBM i5/OS messages	435
Viewing Linux messages	436
Using Service Focal Point	436
Using Service Focal Point for the HMC.	436

Viewing serviceable events	437
Closing serviceable events	437
Viewing serviceable event logical partition information	438
Repairing serviceable events	438
Activating and deactivating LEDs	438
Deactivate a system attention LED or partition LED	438
Activate or deactivate identify LED	439
Setting up connection monitoring	440
Collecting vital product data	440
Using Service Focal Point for the Integrated Virtualization Manager	440
Managing serviceable events with Service Focal Point for the Integrated Virtualization Manager	440
Working with the service utilities on Service Focal Point for the Integrated Virtualization Manager	441
Creating a serviceable event with Service Focal Point for the Integrated Virtualization Manager	441
Managing dumps with Service Focal Point for the Integrated Virtualization Manager	441
Collecting vital product data with Service Focal Point for the Integrated Virtualization Manager	442
Replacing and verifying parts	442
Reporting problems	442
Reporting problems when the HMC is not available	443
Reporting problems when the server is down	443
Using the problem reporting forms	443
Problem reporting form for a system in manufacturing default configuration	443
Problem reporting form for a system with multiple logical partitions	445
Contacting IBM service and support.	447
Related information for Customer service, support, and troubleshooting.	447
Appendix. Accessibility features	451
Notices	453
Trademarks	454
Electronic emission notices	455
Class A Notices.	455
Terms and conditions.	458

Safety and environmental notices

Safety notices may be printed throughout this guide:

- **DANGER** notices call attention to a situation that is potentially lethal or extremely hazardous to people.
- **CAUTION** notices call attention to a situation that is potentially hazardous to people because of some existing condition.
- **Attention** notices call attention to the possibility of damage to a program, device, system, or data.

World Trade safety information

Several countries require the safety information contained in product publications to be presented in their national languages. If this requirement applies to your country, a safety information booklet is included in the publications package shipped with the product. The booklet contains the safety information in your national language with references to the U.S. English source. Before using a U.S. English publication to install, operate, or service this product, you must first become familiar with the related safety information in the booklet. You should also refer to the booklet any time you do not clearly understand any safety information in the U.S. English publications.

Laser safety information

IBM® System i® models and System p® servers can use I/O cards or features that are fiber-optic based and that utilize lasers or LEDs.

Laser compliance

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

CAUTION:

This product might contain one or more of the following devices: CD-ROM drive, DVD-ROM drive, DVD-RAM drive, or laser module, which are Class 1 laser products. Note the following information:

- Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.
- Use of the controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure.

(C026)

CAUTION:

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

CAUTION:

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

CAUTION:

Some laser products contain an embedded Class 3A or Class 3B laser diode. Note the following information: laser radiation when open. Do not stare into the beam, do not view directly with optical instruments, and avoid direct exposure to the beam. (C030)

Power and cabling information for NEBS (Network Equipment-Building System) GR-1089-CORE

The following comments apply to the IBM System i models and IBM System p servers that have been designated as conforming to NEBS (Network Equipment-Building System) GR-1089-CORE:

The equipment is suitable for installation in the following:

- Network telecommunications facilities
- Locations where the NEC (National Electrical Code) applies

The intrabuilding ports of this equipment are suitable for connection to intrabuilding or unexposed wiring or cabling only. The intrabuilding ports of this equipment *must not* be metallically connected to the interfaces that connect to the OSP (outside plant) or its wiring. These interfaces are designed for use as intrabuilding interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE) and require isolation from the exposed OSP cabling. The addition of primary protectors is not sufficient protection to connect these interfaces metallically to OSP wiring.

Note: All Ethernet cables must be shielded and grounded at both ends.

The ac-powered system does not require the use of an external surge protection device (SPD).

The dc-powered system employs an isolated DC return (DC-I) design. The DC battery return terminal *shall not* be connected to the chassis or frame ground.

Product recycling and disposal

This unit must be recycled or discarded according to applicable local and national regulations. IBM encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. IBM offers a variety of product return programs and services in several countries to assist equipment owners in recycling their IT products. Information on IBM product recycling offerings can be found on IBM's Internet site at <http://www.ibm.com/ibm/environment/products/prp.shtml>.

Esta unidad debe reciclarse o desecharse de acuerdo con lo establecido en la normativa nacional o local aplicable. IBM recomienda a los propietarios de equipos de tecnología de la información (TI) que reciclen responsablemente sus equipos cuando éstos ya no les sean útiles. IBM dispone de una serie de programas y servicios de devolución de productos en varios países, a fin de ayudar a los propietarios de equipos a reciclar sus productos de TI. Se puede encontrar información sobre las ofertas de reciclado de productos de IBM en el sitio web de IBM <http://www.ibm.com/ibm/environment/products/prp.shtml>.



EU Only

Note: This mark applies only to countries within the European Union (EU) and Norway.

Appliances are labeled in accordance with European Directive 2002/96/EC concerning waste electrical and electronic equipment (WEEE). The Directive determines the framework for the return and recycling of used appliances as applicable throughout the European Union. This label is applied to various products to indicate that the product is not to be thrown away, but rather reclaimed upon end of life per this Directive.

In accordance with the European WEEE Directive, electrical and electronic equipment (EEE) is to be collected separately and to be reused, recycled, or recovered at end of life. Users of EEE with the WEEE marking per Annex IV of the WEEE Directive, as shown above, must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and recovery of WEEE. Customer participation is important to minimize any potential effects of EEE on the environment and human health due to the potential presence of hazardous substances in EEE. For proper collection and treatment, contact your local IBM representative.

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.

For Taiwan: Please recycle batteries.



For the European Union:



Note: This mark applies only to countries within the European Union (EU).

Batteries or packaging for batteries are labeled in accordance with European Directive 2006/66/EC concerning batteries and accumulators and waste batteries and accumulators. The Directive determines the framework for the return and recycling of used batteries and accumulators as applicable throughout the European Union. This label is applied to various batteries to indicate that the battery is not to be thrown away, but rather reclaimed upon end of life per this Directive.

In accordance with the European Directive 2006/66/EC, batteries and accumulators are labeled to indicate that they are to be collected separately and recycled at end of life. The label on the battery may also include a chemical symbol for the metal concerned in the battery (Pb for lead, Hg for mercury and Cd for cadmium). Users of batteries and accumulators must not dispose of batteries and accumulators as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and treatment of batteries and accumulators. Customer participation is important to minimize any potential effects of batteries and accumulators on the environment and human health due to the potential presence of hazardous substances. For proper collection and treatment, contact your local IBM representative.

For California: Perchlorate Material - special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate.

The foregoing notice is provided in accordance with California Code of Regulations Title 22, Division 4.5 Chapter 33. Best Management Practices for Perchlorate Materials. This product/part may include a lithium manganese dioxide battery which contains a perchlorate substance.

IBM Cryptographic Coprocessor Card Return Program

The following information applies only for systems originally sold prior to July 1, 2006:

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

About this topic

Learn about the tools and options you can use to connect to the service and support organization. If you need to perform manual problem analysis on your server, the troubleshooting information will help you understand, isolate, and resolve problems. Sometimes you will be able to resolve a problem on your own; at other times you will need to gather information to help the service technicians or call center to resolve your problem in a timely manner.

For information about the accessibility features of this product, for users who have a physical disability, see “Accessibility features,” on page 451.

Customer service, support, and troubleshooting

This information helps you to understand and plan for the service and support options based on your requirements. You will learn about the tools and options you can use to connect to the service and support organization. If you need to perform manual problem analysis on your server, the troubleshooting information will help you understand, isolate, and resolve problems. Sometimes you will be able to resolve a problem on your own; at other times you will need to gather information to help the service technicians or call center to resolve your problem in a timely manner.

Your IBM Systems and IBM eServer™ hardware are equipped with tools to help you determine when you need to perform service or call for help. These servers have the capability to either automatically, or under your control, send information to the service and support organization to help them solve your problem.

Also, with your authorization, the system has the capability to allow the service and support organization to remotely connect to your system to assist you with your problem.

Note: If you are using the Integrated Virtualization Manager to manage your server, check Service Focal Point for the Integrated Virtualization Manager to see if you need to contact service and support.

If you need to perform manual problem analysis on your server, the troubleshooting information will help you understand, isolate, and resolve problems. For example, if the system attention light is on, you can find out what it means. For details, see System attention light overview. Also, you can look up reference codes to understand what they mean and actions you can take to resolve them. For details, see Reference code list for customers. Sometimes you will be able to resolve a problem on your own; at other times you will need to gather information to help the service technicians or call center resolve your problem in a timely manner.

Related concepts

“Attention light overview” on page 214

Learn more about the attention light and how you can use it to identify a problem.

“Reference codes list for customers” on page 263

Learn more about the various types of reference codes and how they can help with problem analysis.

What's new for Customer service, support, and troubleshooting

Learn about new or updated information for the Customer service, support, and troubleshooting information

What's new as of September 28, 2007

Updates for managing server firmware updates for i5/OS® with Licensed Internal Code V5R4M5. For details, see “Updates” on page 116.

What's new as of September 2007

Information on using an HMC with Version 7 or later.

PDF file for Customer service, support, and troubleshooting

You can view and print a PDF file of this information.


To view or download the PDF version of this document, select Customer service, support, and troubleshooting (about 6000 KB).

Saving PDF files

To save a PDF file on your workstation for viewing or printing:

1. Right-click the PDF link in your browser.
2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe Reader

You need Adobe Reader installed on your system to view or print these PDFs. You can download a free copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html) .

Overview of service and support

Learn about the service options and the tools available to support your operating environment to ensure that your server and applications are ready when you need them.

The service and support tools described in this topic 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 include:

- Monitoring server and logical partitions
- Outgoing communications with your service and support organization (with correct setup and your authorization)
- Obtaining updates
- Enabling incoming remote support (with correct setup and your authorization)

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

Electronic Service Agent™

An application that can be configured to monitor your systems.

Service Focal Point

An application on the Hardware Management Console (HMC) that is used by service representatives to help diagnose and repair problems on logically partitioned systems.

Remote Support Facility

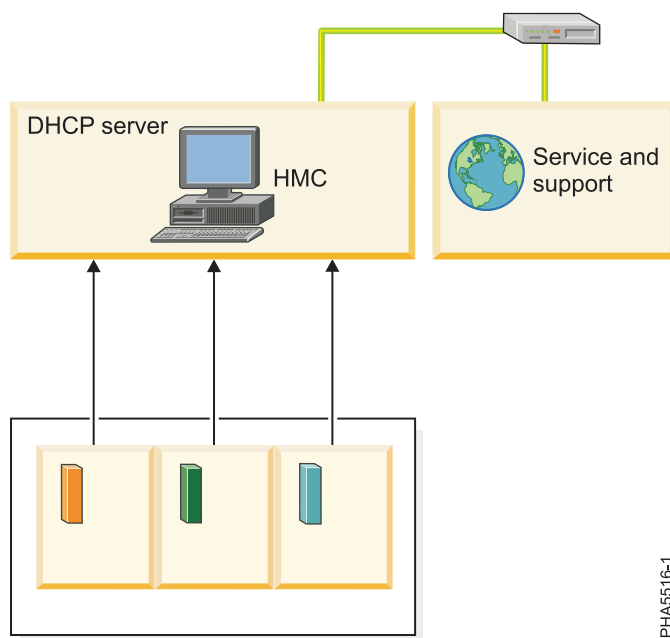
An application that runs on the HMC and enables the HMC to call out to the service and support organization.

Inventory Scout

An application that reports system configuration information and facilitates update of system firmware.

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

Figure 1. The elements of service and support and how they fit together.



IPHA5516-1

In this illustration, three logical partitions run on a server. Each logical partition communicates with the HMC. Then, after you authorize the HMC, the HMC connects to your service and support organization. Your system can be configured to automatically handle these tasks for you, or you might choose to review and individually control them. If the system and applications are enabled, your server can report a problem to the service and support organization without your intervention. If a service representative is needed, you can arrange to have the service performed and to recover from a problem as quickly as possible.

Note: If you are using the Integrated Virtualization Manager to manage your server, check Service Focal Point for the Integrated Virtualization Manager to see if you need to contact service and support.

If your system is not managed by an HMC, there are other tools that can be used to enable your service environment.

For example, the Electronic Service Agent application for the operating system can monitor and analyze a problem and contact the service and support organization if configured. Also, if you have a IBM System p5®, you can configure the Service Processor to monitor the system for problems and to contact service and support when you cannot start the operating system.

Elements of your service environment

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

Connectivity

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

Connectivity from your server or HMC to your service and 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?
- Are there security requirements that you should consider?
- How you plan to connect to your service and support organization (using a console or through the server).

Choosing your connection method:

Learn about choosing your connection method.

Choosing your connection method for AIX or Linux:

Learn about choosing your connection method when you are running AIX® or Linux®.

One of your first tasks is to specify if you want the electronic connection to service and support to be set up and how you will connect. This connection can be through your HMC or, in some cases, through a pass-through system, such as another HMC. When deciding which type of connection to use, consider the following:

Update strategy

The connection type that you select here also dictates how you will install your updates. For example, if you choose to connect to service and support through your HMC, you will install server firmware updates through your HMC.

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

Speed Different connection types offer different rates of data transfer. If you choose to receive data through your electronic connection, try to select the fastest method of sending and receiving data that you have available to you.

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.

Choosing your connection method for i5/OS:

Learn about choosing your connection method when you are running i5/OS.

One of your first tasks is to specify if you want the electronic connection to service and support to be set up and how you will connect. This connection can be through your HMC 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:

Update strategy

The connection type that you select here also dictates how you will install your updates. For example, if you choose to connect to service and support through your HMC, you will install server firmware updates through your HMC.

For i5/OS logical partitions, you can use the usual i5/OS PTF installation functions for installing updates rather than using the HMC. For more information about i5/OS updates, see *Maintaining and managing i5/OS and related software*.

Speed Different connection types offer different rates of data transfer. If you choose to receive data through your electronic connection, try to select the fastest method of sending and receiving data that you have available to you.

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.

Related information

 Maintaining and managing i5/OS and related software

Selecting the order for connectivity:

Learn about selecting the order of connectivity.

An example of the order of connection types by locale and speed is as follows:

Note: You can select multiple methods with automatic fail-over from one connection type to another.

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

The service tools that are provided with your server allow connection to service and support systems with or without the use of an HMC.

For more information about setting up connectivity, see the following topics:

- Scenarios: Service and support
- Setting up your server to connect to service and support
- Specifying the connection type from the HMC

Related concepts

“Scenarios: Service and support” on page 13

These scenarios demonstrate several ways you can connect your server and HMC to the service and support organization.

“Setting up your server to connect to service and support” on page 31

Learn about setting up your server to connect to service and support.

Related tasks

“Specifying the connection type from the HMC” on page 107

Learn how to specify the connection type from the HMC.

Service information

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

Each operating system environment has tools that can help you keep service information about your server. This information can help your service provider or your support organization provide better service and support. Also, you can enable your server to automatically connect to service and support for either outgoing communication, incoming communication, or both.

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, updates, 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 can provide valuable information which can be used by remote service and service representatives so that they can help you keep the firmware and software on your server up to date.

If you choose, 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. For more details, see Electronic Service Agent.

Related concepts

“Electronic Service Agent” on page 9

Learn more about the Electronic Service Agent application which monitors your servers after you enable it.

Electronic problem reporting

Learn about how electronic problem reporting allows you to either automatically or manually notify the service and support organization about any problems that might occur. The information reported can help the support organization provide better service and support.

Your server can help you isolate the cause of most hardware and software problems. If a problem occurs your server can communicate with your service and support organization to help isolate the cause of the problem, if you allow it. 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 and support organization can call you to gather more information and help you perform further problem analysis.
- A service provider can be dispatched to your location.

Note: If you are using the Integrated Virtualization Manager to manage your server, check Service Focal Point for the Integrated Virtualization Manager to see if you need to contact service and support.

For more information about using the service tools, refer to the following information:

- To learn how Electronic Service Agent can help you maintain your system, see Electronic Service Agent.
- To learn how Service Focal Point helps isolate problems that affect multiple logical partitions, see Service Focal Point.
- To learn about the process of setting up the service tools, including Electronic Service Agent and Service Focal Point, for example, see Setting up your service environment.
- To learn about troubleshooting and reporting problems that are not reported electronically, see Getting started with troubleshooting.
- To learn how to report problems to the service and support organization when the automatic reporting process is not available, see Reporting problems.

Related concepts

“Electronic Service Agent” on page 9

Learn more about the Electronic Service Agent application which monitors your servers after you enable it.

“Service Focal Point” on page 10

Learn about the Service Focal Point application, which is used by service representatives to help diagnose and repair problems on logically partitioned systems.

“Setting up your service environment” on page 31

Learn how to set up and configure your server to use the service tools for your operating environment in both an HMC and non-HMC environment.

“Getting started with troubleshooting” on page 212

Learn how you and your server can manage problems, and ways you can detect that problems have occurred.

“Reporting problems” on page 442

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

Updates overview

Learn about ongoing update support and upgrades for your server or HMC and how to obtain software and firmware updates.

Periodically, a problem might be discovered in your server’s software or firmware . When the service and support organization discovers a problem in your software, a software update, sometimes referred to as a *program temporary fix* (PTF), is distributed. If a problem is discovered in the firmware, the update might be released as a PTF or as a firmware update, depending on the server type and model.

Updates 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 update-management strategy to help you keep track of code updates that are available for your software and firmware.

For more details about how to download and install various types of updates, see Updates.

Related concepts

“Updates” on page 116

Learn about obtaining machine code updates for your HMC, server firmware, power subsystem firmware (if you have a model 575 or 59x server), I/O adapter and device, as well as operating system updates.

Remote support

Learn about methods of connecting to your service and support organization to enable either outgoing or incoming remote support, or both.

In some cases, if you agree to permit it, your service and support representatives 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 and authorized the connection.

Virtual private networking (VPN)

This connection type uses several important TCP/IP protocols to protect data traffic.

Secure Sockets Layer (SSL)

SSL has become an industry standard for enabling applications for secure communication sessions over an unprotected network, such as the Internet. SSL uses a cryptographic system that uses two keys to encrypt data, a public key known to everyone and a private or secret key known only to the recipient of the message.

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.

Remote Support Facility (RSF)

This type of connection provides service representatives with diagnostic access to the Licensed Internal Code of the server. If a service representative determines that the RSF method is the best way to diagnose and fix your problem, you will be given detailed information about how to enable the connection.

Note: If you are using the Integrated Virtualization Manager to manage your server, check Service Focal Point for the Integrated Virtualization Manager to see if you need to contact service and support.

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

- To learn how the Remote Support Facility can help you in your service environment, see Remote Support Facility.
- To learn how to enable your system to allow a service representative to remotely perform tasks on your hardware, see Enabling remote support.

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

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

Related concepts

“Remote Support Facility” on page 11

Learn about using the Remote Support Facility, an application that runs on the HMC and enables the HMC to call out to the service and support organization, after you enable it.

“Enable remote support” on page 102

Learn how to set up your server so that you can enable remote support centers to connect and manage your server or your HMC after you permit it.

Related information

Virtual private networking

Start Remote Support (STRRMTSPT) command

Remote Access Services: PPP connections

Using the service applications

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

The service applications are tools that help monitor your server and allow your server to connect to the service and support organization, under your authorization.

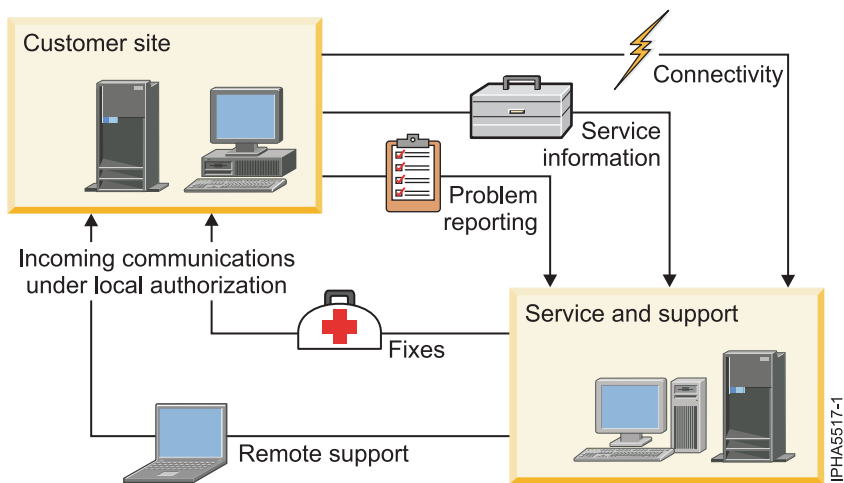
After your server is set up and connected to your service and support organization, the service applications enable service functions to occur automatically. The following applications are related to service and support for your server:

- 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 and support organization.

Figure 2. Service tools and how they work together to help you maintain your server.



The applications that are used to help provide service to your hardware depend on your hardware configuration and your operating environment. If your server is managed with an 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.

Electronic Service Agent

Learn more about the Electronic Service Agent application which monitors your servers after you enable it.

The Electronic Service Agent can run on your server or on an HMC. If Electronic Service Agent is installed and activated 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 with an HMC, 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, either automatically or manually, under your authorization.

Note:

- Serviceable events on the HMC typically consist of problems related to the server firmware and 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 service and support using the appropriate service connection.
- If you are using the Integrated Virtualization Manager to manage your server, check Service Focal Point for the Integrated Virtualization Manager to see if you need to contact service and support.

If enabled, the Electronic Service Agent gateway server 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.

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

For more details on configuring and using Electronic Service Agent on your HMC or server, see Setting up your server to connect to service and support.

For details on using Electronic Service Agent, see the following:

- For AIX or Linux, refer to the Electronic Service Agent Web site at <http://www.ibm.com/support/electronic/navpage?category=5> and search on the appropriate user's guide.
- For i5/OS, refer to the Electronic Service Agent topic in the IBM eServer iSeries Information Center.

Related concepts

"Map of service applications and functions" on page 11

Learn about how each element of your service environment fits together to provide your service solution.

"Setting up your server to connect to service and support" on page 31

Learn about setting up your server to connect to service and support.

Related information



Electronic Service Agent Web site



Electronic Service Agent in the iSeries Information Center

Service Focal Point

Learn about the Service Focal Point application, which is used by service representatives to help diagnose and repair problems on logically partitioned systems.

Service representatives use the Service Focal Point as the starting point for all hardware service issues on logically partitioned systems. The Service Focal Point gathers various hardware system-management issues at one control point, allowing service representatives to use it 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 representatives to avoid long lists of repetitive error 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:

- To find out how Service Focal Point fits into your service environment, see the Map of service applications and functions.
- To find out how you can use Service Focal Point to help you troubleshoot problems, see Using Service Focal Point.

Related concepts

“Map of service applications and functions”

Learn about how each element of your service environment fits together to provide your service solution.

“Using Service Focal Point” on page 436

Learn about using the Service Focal Point, an application on the HMC and the Integrated Virtualization Manager, to diagnose and repair problems on the system.

Remote Support Facility

Learn about using the Remote Support Facility, an application that runs on the HMC and enables the HMC to call out to the service and support organization, after you enable it.

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 representatives to directly access your server, under your authorization and control, 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.

Related concepts

“Map of service applications and functions”

Learn about how each element of your service environment fits together to provide your service solution.

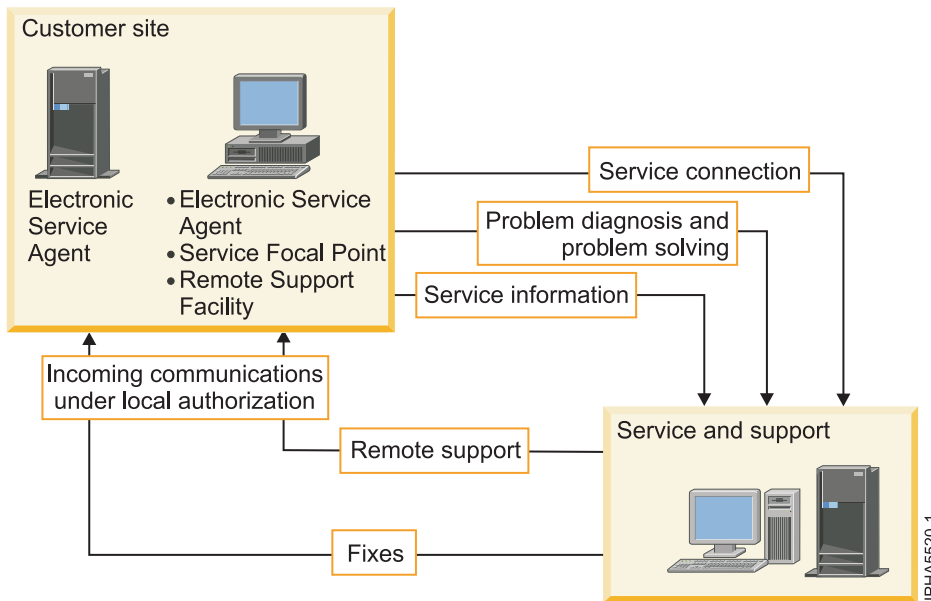
Map of service applications and functions

Learn about how each element of your service environment fits together to provide your service solution.

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.

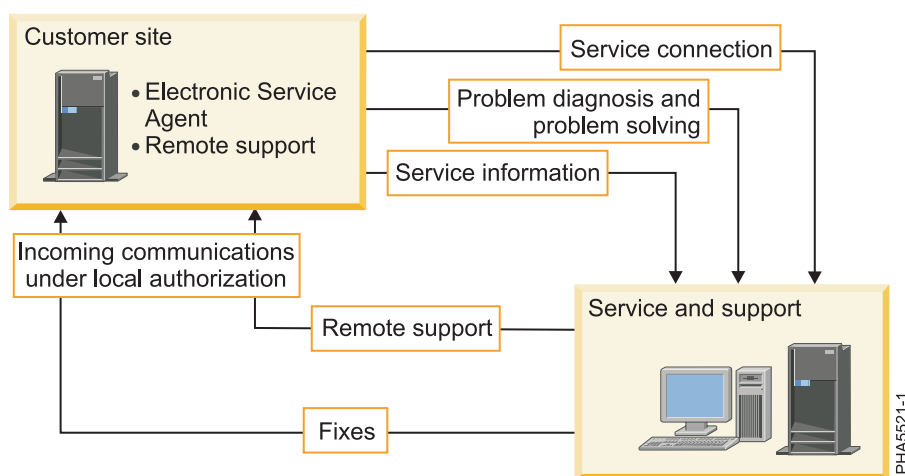
The following illustration shows a server and an HMC at the customer site. Both are connected to the service and support organization. Service applications that run on the server and HMC are displayed beneath each machine in the illustration. These applications perform the service-related functions that are displayed on the directional arrows that run between the customer site and the service and support organization. If you authorize it, the service applications can enable the server and HMC to report problems and service information to the service and support organization. Also, with your approval, the applications can be enabled to allow the service and support organization to provide remote support and to send fixes to your site.

Figure 3. An illustration that shows a server and HMC at the customer site that are connected to the service and support organization. Service applications run on the server and HMC and perform service-related functions. After they are enabled, the applications can allow the server and HMC to report problems and send service information to the service and support organization. Also, with your approval, they can be enabled to allow the service and support organization to provide remote support or to send fixes to your 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 are displayed beneath the server in the illustration. These applications perform the service-related functions that are displayed on the directional arrows between the customer site and the service and support organization. If you authorize it, the service applications can enable the server to report problems and send service information to the service and support organization. Also, with your approval, they can be enabled to allow the service and support organization to provide remote support or to send fixes to your site.

Figure 4. An illustration that shows a server at the customer site that is connected to the service and support organization. Service applications run on the server and perform service-related functions. If you authorize it, the applications can enable the server to report problems and send service information to the service and support organization. Also, with your approval, they can be enabled to allow the service and support organization to provide remote support or to send fixes to your site.



Note: If you are using the Integrated Virtualization Manager to manage your server, check Service Focal Point for the Integrated Virtualization Manager to see if you need to contact service and support.

Scenarios: Service and support

These scenarios demonstrate several ways you can connect your server and HMC to the service and support organization.

Note: In these scenarios, it is assumed that you have enabled automatic connection to service and support. It is possible (although not recommended) for you to maintain manual control of each electronic connection by requiring manual authorization of each system attempt to connect electronically.

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 on the HMC to install your service tools. If you do not have an HMC, you can set up your service tools manually.

Compare the 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.

If you are running AIX in a full system partition profile on a single server, or in multiple logical 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 service and support.

Note: If you are using the Integrated Virtualization Manager to manage your server, check Service Focal Point for the Integrated Virtualization Manager to see if you need to contact service and support.

Scenario: Multiple AIX logical partitions with an HMC

Learn how to connect your AIX logical partitions to enable service features on your server and your HMC.

Situation

If you are responsible for maintaining servers at your company, one of your roles might be to establish the connections within your network and to the service and support organization so that your servers can access service and support resources. For this scenario, you are using an HMC to manage your server and you are planning for four logical partitions.

Objectives

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

- To set up the HMC to connect to service and support
- Ensure that the logical partitions communicate to the HMC.

Also, in this scenario, you want to set up an additional connection from the server to report software problems to service and support. The objectives are as follows:

- To set up the modem on a logical partition to connect to service and support

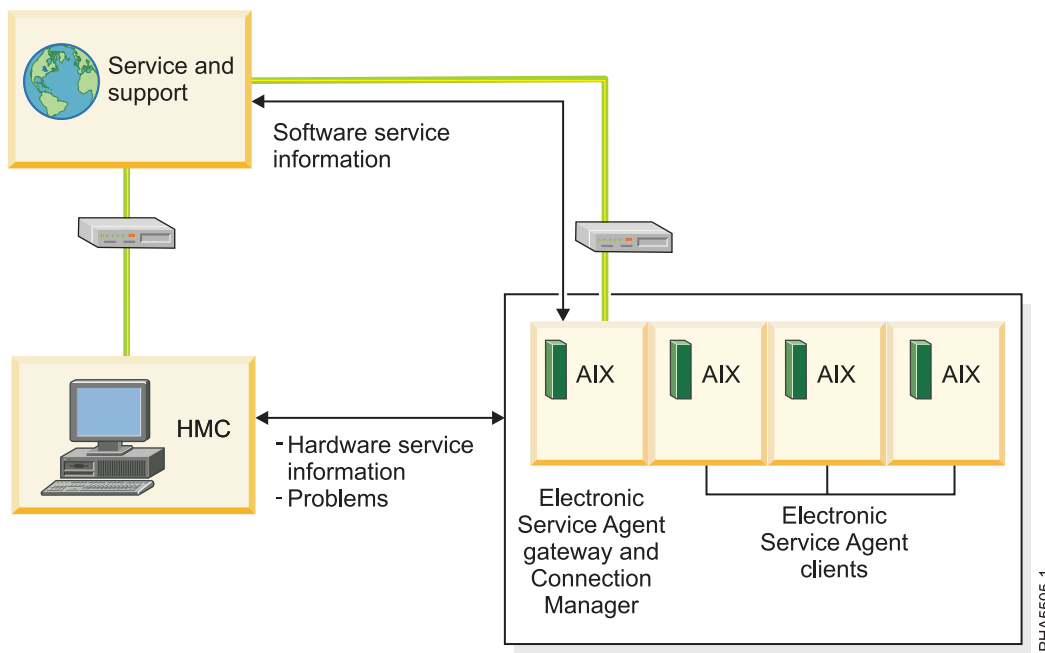
Note: Alternatively, you can use a direct Internet connection.

- To configure Electronic Service Agent on the logical partition that has a modem to be the Electronic Service Agent gateway server
- To configure Electronic Service Agent on other logical partitions to be Electronic Service Agent clients and to communicate with the Electronic Service Agent gateway server

Details

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

Figure 5. A figure showing an HMC and managed system with four logical partitions and their connections to service and support through the HMC modem and through the modem on the server.



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 service and support.

Note: Alternatively, you can use a direct Internet connection.

- 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 Electronic Service Agent gateway server and Connection Manager are set up on a logical partition with a modem that connects to service and support.
- The Electronic Service Agent clients are set up on three other logical partitions.
- Hardware service information and problems flow from each logical partition to service and support using the modem on the HMC, as follows: AIX partition > HMC > Service and support

- Software service information flows from each logical partition to service and support using the modem on the server, as follows: AIX partitions (Electronic Service Agent clients) > AIX partition (Electronic Service Agent gateway server) > Service and support

Prerequisites and assumptions

Successful implementation of this scenario requires that all necessary hardware planning and setup tasks are complete.

Configuration steps

You must complete the following tasks:

1. Ensure that all prerequisites are met for your connection method. Refer to “Task 3. Prerequisites” on page 49.
2. Ensure that your physical networking is set up correctly. See “Task 4. Ensure that your physical networking is set up correctly” on page 49.
3. Obtain or verify your IBM ID. See “Task 5. Obtain or verify an IBM ID” on page 51.
4. Set up the HMC to connect to service and support. You can use either of the following methods to set up the HMC.
 - **Guided Setup wizard** (recommended method): The Guided Setup wizard is a tool on the HMC designed to guide you through the steps of setting up the HMC, including connectivity from the HMC to service and support.
Although you typically use the Guided Setup wizard when you first set up your server, you can also use it to verify that your connections from the HMC to service and support are set up correctly. For details, see “Task 6. Verify the HMC service settings” on page 52.
 - **Manual setup**: If you prefer to use the manual method to create your service connections from the HMC to service and support, see “Manually set up the HMC to connect to service and support” on page 104.
5. Set up and configure the logical partitions. For details, refer to the Partitioning the server topic.
6. Install the operating system on your logical partitions. For details, refer to Installing operating systems.
7. Configure your TCP/IP network. For instructions, refer to the operating system documentation.
8. Activate TCP/IP on your logical partitions. TCP/IP starts automatically, as long as the network adapter is recognized and can communicate with the network when the AIX operating system is started.
9. *Optional*: Obtain and configure Electronic Service Agent to enable the partitions to connect to the software service and support organization.
If you have an HMC, you do not need to obtain and configure Electronic Service Agent for AIX or Linux. The AIX and Linux inventory and hardware-problem information (or report, perhaps) are sent through the HMC. However, you might want to set up Electronic Service Agent on AIX or Linux to contact the software service organization.
 - a. Obtain and configure Electronic Service Agent on AIX. See “Task 11. Obtain and configure Electronic Service Agent for AIX or Linux” on page 54.
 - b. Use the Service Agent (SA) Basic User Interface. See “Task 12. Use the Service Agent (SA) Basic User Interface” on page 56.
 - c. Register the IBM ID. See “Task 13. Register the ID with Electronic Service Agent for AIX or Linux” on page 57.
10. Configure the service processor. See “Task 14. Configure the service processor” on page 57.
11. Verify that the connection to service and support is set up correctly and that information is being transmitted correctly. See “Task 15. Test the connection to service and support” on page 58.

12. View information that was shared with IBM. See “Task 16. View the server information that was reported” on page 59.

Related tasks

“Specifying the connection type from the HMC” on page 107

Learn how to specify the connection type from the HMC.

Scenario: Multiple servers running AIX without an HMC

Learn how to connect one server or multiple servers in a configuration that enables service features.

Situation

If you are responsible for maintaining servers at your company, one of your roles might be to establish the connections within your network and to the service and support organization so that your servers can access service and support resources. For this scenario, you are using a modem that is attached to one of your servers to communicate with service and support.

Note: If you are using the Integrated Virtualization Manager to manage your server, check Service Focal Point for the Integrated Virtualization Manager to see if you need to contact service and support.

Objectives

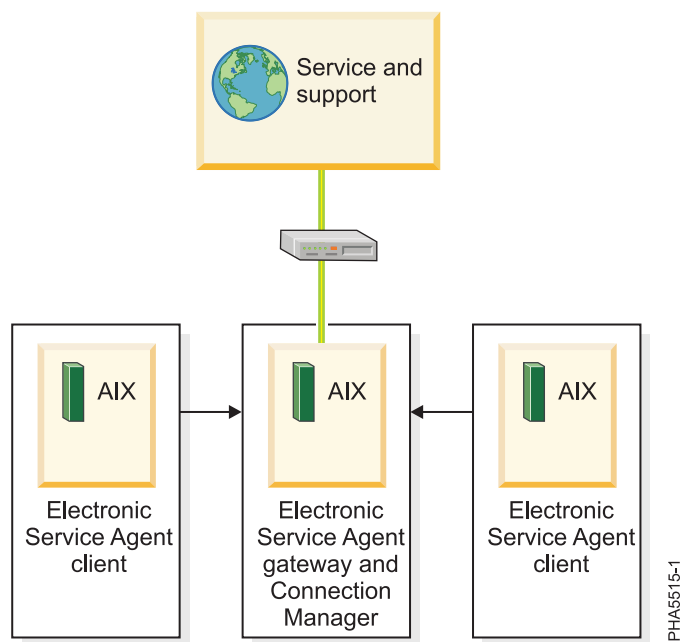
In this scenario, you want to ensure that your servers are connected to service and support so that support is available to the your network administrator. The objectives of this scenario are as follows:

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

Note: Alternatively, you can use an Internet connection instead of the modem to connect to service and support.

- To configure Electronic Service Agent on the other client servers to communicate with the server that has the modem

Figure 6. The following figure illustrates the flow of service information and problems through the service connection from the servers to service and support.



The figure illustrates the following points relevant to this scenario:

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

Prerequisites and assumptions

Successful implementation of this scenario requires that all necessary hardware planning and setup tasks are complete.

Configuration steps

You must complete the following tasks:

1. Ensure that all prerequisites are met for your connection method. Refer to “Task 3. Prerequisites” on page 60.
2. Ensure that your physical networking is set up correctly. Refer to “Task 4. Ensure that your physical network is set up correctly” on page 60.
3. Obtain or verify your IBM ID. See “Task 5. Obtain or verify an ID” on page 60.
4. Install the operating system on your servers. For details, see Installing operating systems.
5. Configure your TCP/IP network. For instructions, refer to the operating system documentation.
6. Activate TCP/IP on your server. TCP/IP starts automatically, as long as the network adapter is recognized and can communicate with the network when the AIX operating system is started.
7. Obtain Electronic Service Agent, and configure it on the gateway server and the client servers by performing these tasks:
 - a. Obtain and configure Electronic Service Agent for AIX. See “Task 9. Obtain and configure Electronic Service Agent for AIX or Linux” on page 61.
 - b. Use the Service Agent (SA) Basic User Interface. See “Task 10. Use the Service Agent (SA) Basic User Interface” on page 64.

- c. Register the IBM ID with Electronic Service Agent for AIX. See “Task 11. Register the ID with Electronic Service Agent for AIX or Linux” on page 64.
8. Configure the service processor for connectivity. See “Task 12. Configure the service processor” on page 64.
9. Verify that the connection to service and support is set up correctly and that information is being transmitted correctly. See “Task 13. Test the connection to service and support” on page 65.
10. View information that was shared. See “Task 14. View the server information that was reported” on page 66.

Scenarios: IBM i5/OS

If you are running the i5/OS operating system, learn about the most common service scenarios for connecting i5/OS to service and support.

Review the scenarios to become familiar with the technical and configuration details. Find the connectivity method that works best with the hardware you use.

Scenario: Multiple IBM i5/OS logical partitions using a direct Internet connection on an i5/OS logical partition

Learn how to configure multiple logical partitions to connect to service and support through a direct Internet connection on an i5/OS logical partition.

Situation

If you are responsible for maintaining servers at your company, one of your roles might be to establish the connections within your network to the service and support organization so that your servers can 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

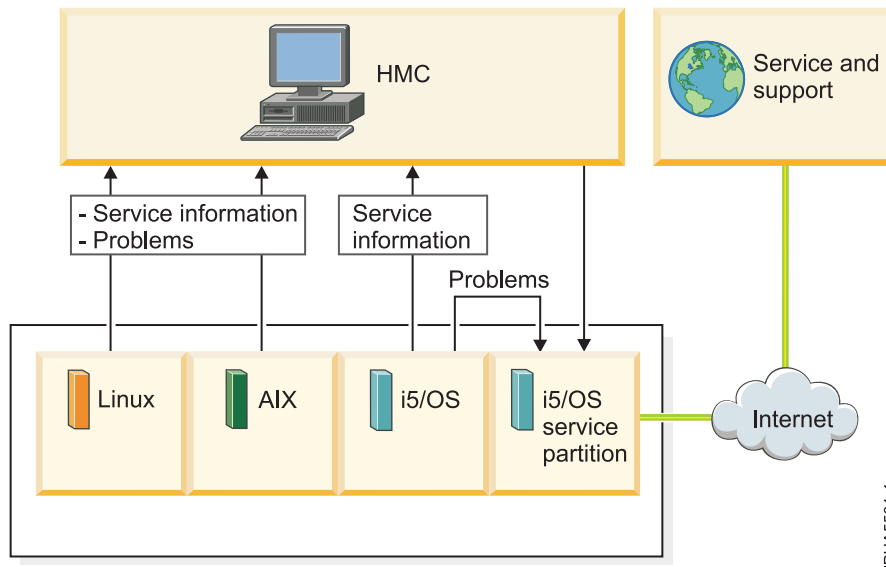
In this scenario, you want to ensure that your company’s server can receive support from the service organization when requested by your company’s network administrator. The objectives of this scenario are as follows:

- To set up the HMC to connect to service and support through the direct Internet connection on the i5/OS partition
- To create a direct Internet 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 information and problems through the service connection to service and support.

Figure 7. This diagram shows the flow of information and problems from four logical partitions and the HMC to service and support. The information and problems pass through the direct Internet connection on the i5/OS logical partition.



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 direct Internet connection is configured on the service partition and connects to service and support.
- Service information and problems flow from each logical partition to service and support using either an HTTPs or 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 all necessary hardware planning and setup tasks are complete.

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

Configuration steps

You must complete the following tasks:

1. Ensure that all prerequisites are met for your connection method. Refer to “Task 3. Prerequisites” on page 67.

2. Ensure that your physical networking is set up correctly. See “Task 4. Ensure that your physical networking is set up correctly” on page 68.
3. Obtain or verify your IBM ID. See “Task 5. Obtain or verify an IBM ID” on page 69.
4. Set up the HMC to connect to service and support. You can use either of the following methods to set up the HMC.
 - **Guided Setup wizard** (recommended method): The Guided Setup wizard is a tool on the HMC designed to guide you through the steps of setting up the HMC, including connectivity from the HMC to service and support. Although you typically use the Guided Setup wizard when you first set up your server, you can also use it to verify that your connections from the HMC to service and support are set up correctly. For details, see “Task 6. Verify the HMC service settings” on page 69.
 - **Manual setup**: If you prefer to use the manual method to create your service connections from the HMC to service and support, see “Manually set up the HMC to connect to service and support” on page 104.
5. Set up and configure the logical partitions. For details, refer to the Partitioning the server topic.
6. Install i5/OS on your system or logical partitions. For details, refer to Installing operating systems.
7. Configure your TCP/IP network. For instructions, refer to the operating system documentation.
8. Activate TCP/IP on your logical partitions. TCP/IP starts automatically, as long as the network adapter is recognized and can communicate with the network when the i5/OS operating system is started.

Note: If TCP/IP does not activate, type STRTCP at an i5/OS command line to start TCP/IP. This command initializes and activates TCP/IP processing, starts the TCP/IP interfaces, and starts the server jobs. Only TCP/IP interfaces and servers with AUTOSTART *YES are started with the STRTCP command.

9. Create a shared direct Internet (HTTP(S) or VPN) connection from the i5/OS logical partitions. See “Task 11. Configure Electronic Service Agent for i5/OS” on page 71.
10. Register the IBM ID for i5/OS. See “Task 12. Register the IBM ID for i5/OS” on page 76.
11. Verify that the connection to service and support is set up correctly and that information is being transmitted correctly. See “Task 13. Test the connection to service and support” on page 76.
12. View information that was shared with IBM. See “Task 14. View the server information that was reported to IBM” on page 77.

Related tasks

“Specifying the connection type from the HMC” on page 107
 Learn how to specify the connection type from the HMC.

Scenario: Multiple IBM i5/OS logical partitions using the HMC’s modem

Learn how to configure multiple logical partitions to connect to service and support through the modem on the HMC.

Situation

If you are responsible for maintaining servers at your company, one of your roles might be to establish the connections within your network and to the service and support organization so that your servers can 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

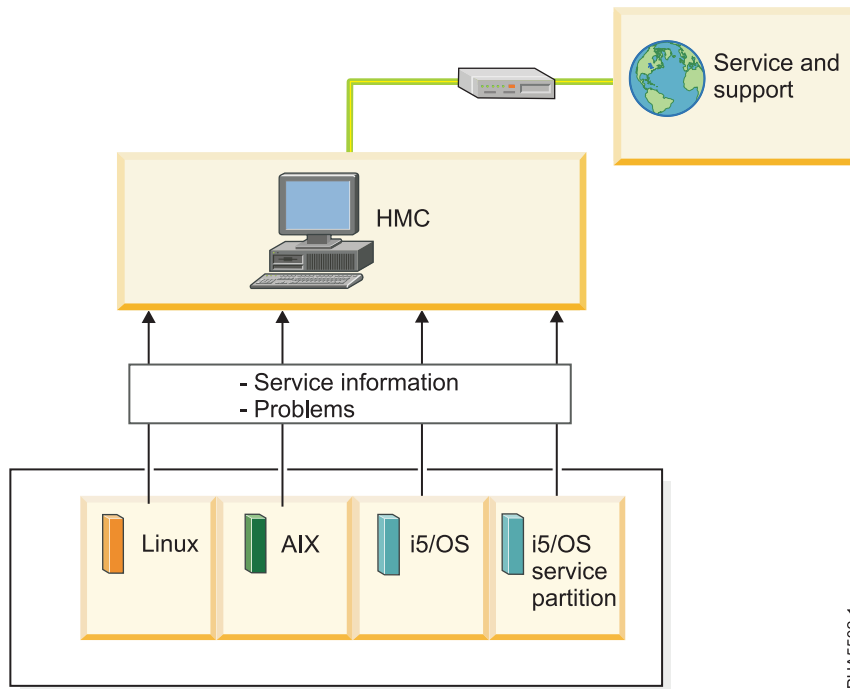
In this scenario, you want to ensure that your company’s server can receive support from the service organization when requested by your company’s network administrator. The objectives of this scenario are as follows:

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

Details

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

Figure 8. This diagram shows the flow of information and problems from four logical partitions and the HMC to service and support. The information and problems pass through the PPP connection on the HMC.



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 service and support.
- Service information and problems flow from each logical partition to service and support 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 all necessary hardware planning and setup tasks are complete. Additional prerequisites and assumptions are noted in the appropriate places within the configuration tasks.

Configuration steps

You must complete the following tasks:

1. Ensure that all prerequisites are met for your connection method. Refer to “Task 3. Prerequisites” on page 67.
2. Ensure that your physical networking is set up correctly. See “Task 4. Ensure that your physical networking is set up correctly” on page 68.
3. Obtain or verify your IBM ID. See “Task 5. Obtain or verify an IBM ID” on page 69.
4. Set up the HMC to connect to service and support. You can use either of the following methods to set up the HMC.
 - **Guided Setup wizard** (recommended method): The Guided Setup wizard is a tool on the HMC designed to guide you through the steps of setting up the HMC, including connectivity from the HMC to service and support. Although you typically use the Guided Setup wizard when you first set up your server, you can also use it to verify that your connections from the HMC to service and support are set up correctly. For details, see “Task 6. Verify the HMC service settings” on page 69.
 - **Manual setup**: If you prefer to use the manual method to create your service connections from the HMC to service and support, see “Manually set up the HMC to connect to service and support” on page 104.
5. Set up and configure the logical partitions. For details, refer to the Partitioning the server topic.
6. Install i5/OS on your system or logical partitions. For details, refer to Installing operating systems.
7. Configure your TCP/IP network. For instructions, refer to the operating system documentation.
8. Activate TCP/IP on your logical partitions. TCP/IP starts automatically, as long as the network adapter is recognized and can communicate with the network when the i5/OS operating system is started.

Note: If TCP/IP does not activate, type STRTCP at an i5/OS command line to start TCP/IP. This command initializes and activates TCP/IP processing, starts the TCP/IP interfaces, and starts the server jobs. Only TCP/IP interfaces and servers with AUTOSTART *YES are started with the STRTCP command.

9. Configure each logical partition to use the modem on the HMC to connect to service and support. See “Task 11. Configure Electronic Service Agent for i5/OS” on page 71.
10. Register the IBM ID for i5/OS. See “Task 12. Register the IBM ID for i5/OS” on page 76.
11. Verify that the connection to service and support is set up correctly and that information is being transmitted correctly. See “Task 13. Test the connection to service and support” on page 76.
12. View information that was shared with IBM. See “Task 14. View the server information that was reported to IBM” on page 77.

Related tasks

“Specifying the connection type from the HMC” on page 107
Learn how to specify the connection type from the HMC.

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

Learn how to configure multiple logical partitions to connect to service and support through the modem on an i5/OS logical partition.

Situation

If you are responsible for maintaining servers at your company, one of your roles might be to establish the connections within your network and to the service and support organization so that your servers can 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

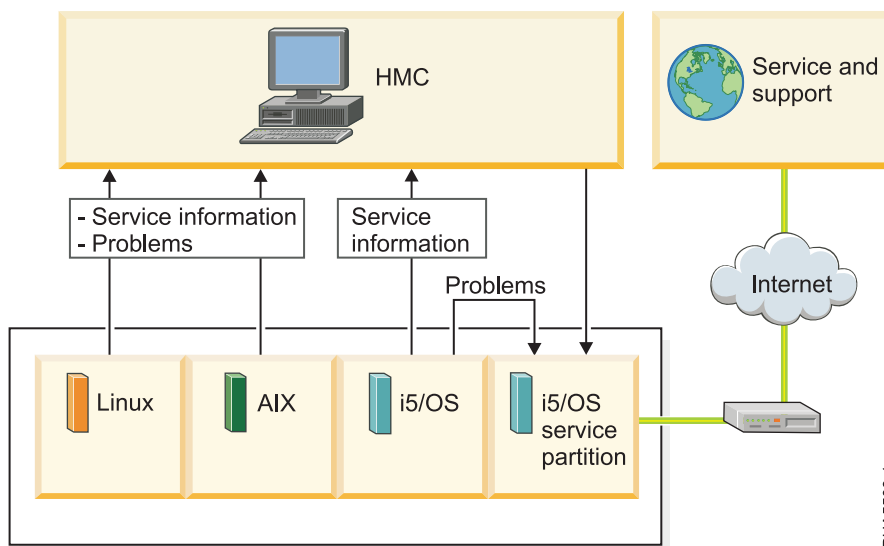
In this scenario, you want to ensure that your company's server can receive support from the service organization when requested by your company's network administrator. The objectives of this scenario are as follows:

- To set up the HMC to connect to service and support
- To configure the i5/OS logical partition that has the modem for dial-up connection to service and support
- 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 service and support.

Figure 9. This diagram shows the flow of information and problems from four logical partitions and the HMC to service and support. The information and problems pass through the PPP connection on the i5/OS logical partition.



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 service and support.
- Service information and problems flow from each logical partition to service and support 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 all necessary hardware planning and setup tasks are complete. Additional prerequisites and assumptions are noted in the appropriate places within the configuration tasks.

Configuration steps

You must complete the following tasks:

1. Ensure that all prerequisites are met for your connection method. Refer to “Task 3. Prerequisites” on page 67.
2. Ensure that your physical networking is set up correctly. See “Task 4. Ensure that your physical networking is set up correctly” on page 68.
3. Obtain or verify your IBM ID. See “Task 5. Obtain or verify an IBM ID” on page 69.
4. Set up the HMC to connect to service and support. You can use either of the following methods to set up the HMC.
 - **Guided Setup wizard** (recommended method): The Guided Setup wizard is a tool on the HMC designed to guide you through the steps of setting up the HMC, including connectivity from the HMC to service and support. Although you typically use the Guided Setup wizard when you first set up your server, you can also use it to verify that your connections from the HMC to service and support are set up correctly. For details, see “Task 6. Verify the HMC service settings” on page 69.
 - **Manual setup**: If you prefer to use the manual method to create your service connections from the HMC to service and support, see “Manually set up the HMC to connect to service and support” on page 104.
5. Set up and configure the logical partitions. For details, refer to the Partitioning the server topic.
6. Install i5/OS on your system or logical partitions. For details, refer to Installing operating systems.
7. Configure your TCP/IP network. For instructions, refer to the operating system documentation.
8. Activate TCP/IP on your logical partitions. TCP/IP starts automatically, as long as the network adapter is recognized and can communicate with the network when the i5/OS operating system is started.

Note: If TCP/IP does not activate, type STRTCP at an i5/OS command line to start TCP/IP. This command initializes and activates TCP/IP processing, starts the TCP/IP interfaces, and starts the server jobs. Only TCP/IP interfaces and servers with AUTOSTART *YES are started with the STRTCP command.

9. Configure a shared modem connection from the i5/OS logical partitions. See “Task 11. Configure Electronic Service Agent for i5/OS” on page 71.
10. Register the IBM ID for i5/OS. See “Task 12. Register the IBM ID for i5/OS” on page 76.
11. Verify that the connection to service and support is set up correctly and that information is being transmitted correctly. See “Task 13. Test the connection to service and support” on page 76.
12. View information that was shared with IBM. See “Task 14. View the server information that was reported to IBM” on page 77.

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

Learn how to configure multiple i5/OS logical partitions to connect to service and support through the modem on the i5/OS logical partition and to enable the HMC to connect to service and support 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 service and support. Or, in the event the i5/OS modem is busy or unavailable, it can use the modem on the HMC to connect to service and support.

Situation

If you are responsible for maintaining servers at your company, one of your roles might be to establish the connections within your network and to the service and support organization so that your servers can access service and support resources. For this scenario, 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 service and support. 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 service and support.

Objectives

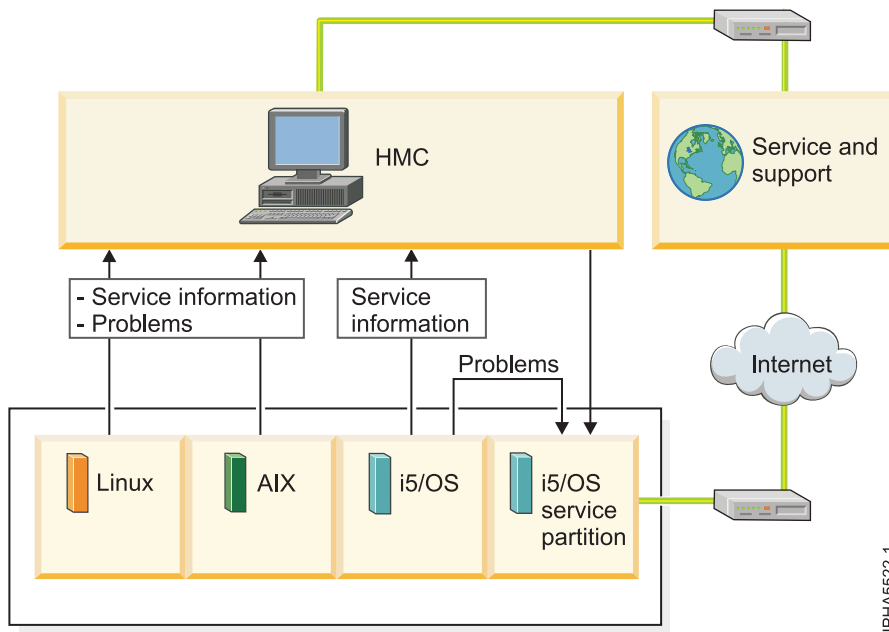
In this scenario, you want to ensure that your company's server can receive support from the service organization when requested by your company's network administrator. The objectives of this scenario are as follows:

- To set up the HMC to connect to 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 service and support, and as a backup, to use the HMC modem
- To configure the i5/OS logical partition that has the modem for dial-up connection to service and support, and as a backup, to use the HMC modem
- 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 service and support

Details

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

Figure 10. This diagram shows the flow of information and problems from four logical partitions and the HMC to service and support. The information and problems pass through the modem on the HMC or through the modem on the i5/OS logical partition.



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 service and support.
- The logical partitions use either the modem on the HMC or the modem on the service partition to connect to service and support.
- Service information and problems flow from each logical partition to service and support 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 logical partition > HMC > Service and support (backup)
 - i5/OS service partition > Service and support
 - i5/OS service partition > HMC > Service and support (backup)

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 service and support.

Prerequisites and assumptions

Successful implementation of this scenario requires that all necessary hardware planning and setup tasks are complete. Additional prerequisites and assumptions are noted in the appropriate places within the configuration tasks.

Configuration steps

You must complete the following tasks:

1. Ensure that all prerequisites are met for your connection method. Refer to “Task 3. Prerequisites” on page 67.
2. Ensure that your physical networking is set up correctly. See “Task 4. Ensure that your physical networking is set up correctly” on page 68.
3. Obtain or verify your IBM ID. See “Task 5. Obtain or verify an IBM ID” on page 69.
4. Set up the HMC to connect to service and support. You can use either of the following methods to set up the HMC.
 - **Guided Setup wizard** (recommended method): The Guided Setup wizard is a tool on the HMC designed to guide you through the steps of setting up the HMC, including connectivity from the HMC to service and support. Although you typically use the Guided Setup wizard when you first set up your server, you can also use it to verify that your connections from the HMC to service and support are set up correctly. For details, see “Task 6. Verify the HMC service settings” on page 69.
 - **Manual setup**: If you prefer to use the manual method to create your service connections from the HMC to service and support, see “Manually set up the HMC to connect to service and support” on page 104.
5. Set up and configure the logical partitions. For details, refer to the Partitioning the server topic.
6. Install i5/OS on your system or logical partitions. For details, refer to Installing operating systems.
7. Configure your TCP/IP network. For instructions, refer to the operating system documentation.
8. Activate TCP/IP on your logical partitions. TCP/IP starts automatically, as long as the network adapter is recognized and can communicate with the network when the i5/OS operating system is started.

Note: If TCP/IP does not activate, type STRTCP at an i5/OS command line to start TCP/IP. This command initializes and activates TCP/IP processing, starts the TCP/IP interfaces, and starts the server jobs. Only TCP/IP interfaces and servers with AUTOSTART *YES are started with the STRTCP command.

9. Configure PPP connection from the i5/OS service partition to report i5/OS problems to service and support. See “Task 11. Configure Electronic Service Agent for i5/OS” on page 71.
10. Configure PPP connections from the i5/OS logical partitions to use the modem on the service partition to report i5/OS problems to service and support. See “Task 11. Configure Electronic Service Agent for i5/OS” on page 71.
11. Make sure that the HMC modem is set up to allow use by the logical partitions.
12. Register the IBM ID for i5/OS. See “Task 12. Register the IBM ID for i5/OS” on page 76.
13. Verify that the connection to service and support is set up correctly and that information is being transmitted correctly. See “Task 13. Test the connection to service and support” on page 76.
14. View information that was shared with IBM. See “Task 14. View the server information that was reported to IBM” on page 77.

Scenario: IBM i5/OS without an HMC using direct Internet

Learn how to configure i5/OS to use a direct Internet to connect to service and support when you do not use an HMC to manage your system.

Situation

If you are responsible for maintaining servers at your company, one of your roles might be to establish the connections within your network and to the service and support organization so that your servers can access service and support resources.

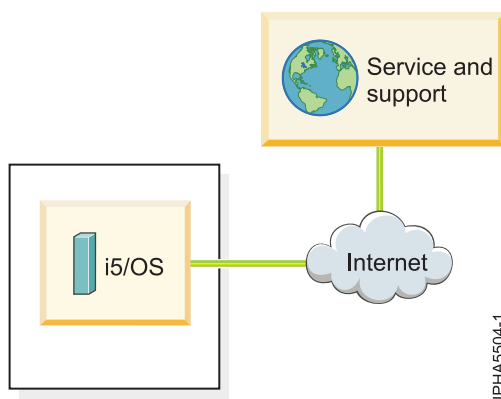
Objectives

In this scenario, you want to ensure that your company's server can receive support from the service organization when requested by your company's network administrator. The objective of this scenario is to create a direct Internet connection from the server to service and support.

Details

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

Figure 11. This diagram shows the flow of information and problems from a server in its manufacturing default configuration to service and support. The information and problems pass through the direct Internet connection on the server.



The figure illustrates the following points relevant to this scenario:

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

Prerequisites and assumptions

Successful implementation of this scenario requires that all necessary hardware planning and setup tasks 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. Ensure that all prerequisites are met for your connection method. Refer to "Task 3. Prerequisites" on page 78.
2. Ensure that your physical networking is set up correctly. See "Task 4. Ensure that your physical networking is set up correctly" on page 78.
3. Obtain or verify your IBM ID. See "Task 5. Obtain or verify an IBM ID" on page 79.
4. Install i5/OS on your system or logical partitions. For details, refer to Installing operating systems.
5. Configure your TCP/IP network. For instructions, refer to the operating system documentation.
6. Activate TCP/IP on your logical partitions. TCP/IP starts automatically, as long as the network adapter is recognized and can communicate with the network when the i5/OS operating system is started.

Note: If TCP/IP does not activate, type STRTCP at an i5/OS command line to start TCP/IP. This command initializes and activates TCP/IP processing, starts the TCP/IP interfaces, and starts the server jobs. Only TCP/IP interfaces and servers with AUTOSTART *YES are started with the STRTCP command.

7. Configure a direct connection to service and support from the server. See “Task 9. Configure Electronic Service Agent for i5/OS” on page 79.
8. Register the IBM ID for i5/OS. See “Task 10. Register the IBM ID for i5/OS” on page 83.
9. Verify that the connection to service and support is set up correctly and that information is being transmitted correctly. See “Task 11. Test the connection to service and support” on page 83.
10. View information that was reported to IBM. See “Task 12. View the server information that was reported to IBM” on page 83.

Scenario: Linux without an HMC

Learn about the most common service scenario for Linux.

Situation

If you are responsible for maintaining servers at your company, one of your roles might be to establish the connections within your network and to the service and support organization so that your servers can access service and support resources.

Objectives

In this scenario, you want to ensure that your company’s server can receive support from the service organization when requested by your 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 service and support

Note: Alternatively, you can use an Internet connection instead of the modem to connect to service and support.

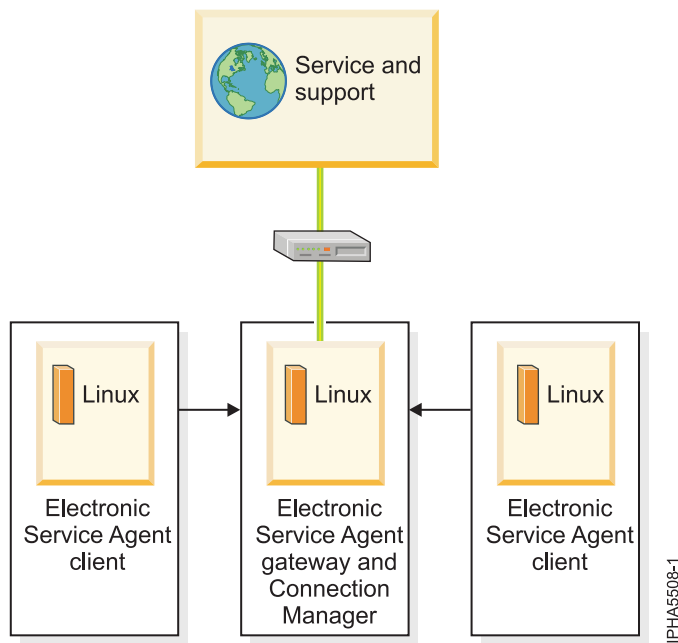
- To configure Electronic Service Agent on the other client servers to communicate with the server that has the modem

Note: If you are using the Integrated Virtualization Manager to manage your server, check Service Focal Point for the Integrated Virtualization Manager to see if you need to contact service and support.

Details

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

Figure 12. A figure of three Linux servers and their connection through a modem to service and support.



The figure illustrates the following points relevant to this scenario.

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

Prerequisites and assumptions

Successful implementation of this scenario requires that all necessary hardware planning and setup tasks are complete.

Configuration steps

You must complete the following tasks:

1. Ensure that all prerequisites are met for your connection method. Refer to “Task 3. Prerequisites” on page 60.
2. Ensure that your physical networking is set up correctly. Refer to “Task 4. Ensure that your physical network is set up correctly” on page 60.
3. Obtain or verify your IBM ID. See “Task 5. Obtain or verify an ID” on page 60.
4. Install the operating system on your servers. For details, see Installing operating systems.
5. Configure your TCP/IP network. For instructions, refer to the operating system documentation.
6. Activate TCP/IP on your server. TCP/IP starts automatically, as long as the network adapter is recognized and can communicate with the network when the AIX operating system is started.
7. Obtain Electronic Service Agent, and configure it on the gateway server and the client servers by performing these tasks:
 - a. Obtain and configure Electronic Service Agent for AIX. See “Task 9. Obtain and configure Electronic Service Agent for AIX or Linux” on page 61.

- b. Use the Service Agent (SA) Basic User Interface. See “Task 10. Use the Service Agent (SA) Basic User Interface” on page 64.
 - c. Register the IBM ID with Electronic Service Agent for AIX. See “Task 11. Register the ID with Electronic Service Agent for AIX or Linux” on page 64.
8. Configure the service processor for connectivity. See “Task 12. Configure the service processor” on page 64.
 9. Verify that the connection to service and support is set up correctly and that information is being transmitted correctly. See “Task 13. Test the connection to service and support” on page 65.
 10. View information that was shared. See “Task 14. View the server information that was reported” on page 66.

Setting up your service environment

Learn how to set up and configure your server to use the service tools for your operating environment in both an HMC and non-HMC environment.

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

- HMC
- System console
- PC that is able to connect to the Advanced System Management Interface (ASMI)

For details, see Requirements needed by service personnel.

Related concepts

“Requirements needed by service personnel” on page 104

Learn about the requirements that the service personnel need to have available when they service your systems.

Setting up your server to connect to service and support

Learn about setting up your server to connect to service and support.

After you have configured your HMC (if you have one), you must set up the connection to service and support from your server. This connection can provide two-way communication between your server and service and support. Each operating environment has requirements to consider when you set up your connections.

Setting up a 7037-A50 or a 7047-185 system to connect to service and support

Learn about all the tasks you need to perform to set up connectivity to service and support when you are working on a 7037-A50 or a 7047-185 system.

Perform or verify Tasks 1 through 13 to set up connectivity for a 7037-A50 or a 7047-185 system.

Task 1. Before you begin:

This procedure contains the complete list of tasks needed to set up connectivity to service and support. Some of these tasks might already have been completed (during initial server setup, for example). If so, you can use this procedure to verify that the tasks were completed correctly.

In this document, an *Internet connection* is defined as access to the Internet from a logical partition or server by direct or indirect access. *Indirect* means that you are behind a Network Address Translation (NAT) firewall. *Direct* means that you have a globally routable address without an intervening firewall, which would block the ports that are needed for communication to service and support.

Task 2. Decide on your connectivity method:

Use one of the following, depending on your situation:

- Internet connection over Secure Sockets Layer (SSL), default configuration
- Direct or shared (if more than one server) dial-up connection over SSL

Task 3. Prerequisites:

Depending on your situation, complete one of the following:

- For IBM System p5 or IBM eServer p5 servers, choose from the following options:
 - If an HTTP proxy is available within your network, then the Service Agent traffic can be routed to it by specifying the Proxy Type as HTTP and Proxy Port as 80.
 - If HTTPS traffic is restricted, ensure that the following port is open for communication: Protocol TCP port 443 with the following IP addresses: 207.25.252.200 and 129.42.160.48
- For dial-up (modem) connection, determine necessary configuration settings, including:
 - Local area code
 - Predial information, such as dialing 9 to dial outside the network
 - Use of commas if delayed dialing is needed
 - Point to Point Protocol (PPP) required for dial connection
 - Available tty or vty devices

Task 4. Ensure that your physical networking is set up correctly:

Verify the physical connection from your site to service and support. This connection enables you to report hardware problems and other server information to service and support. It also enables you to install updates. This connection is represented in the following illustration:

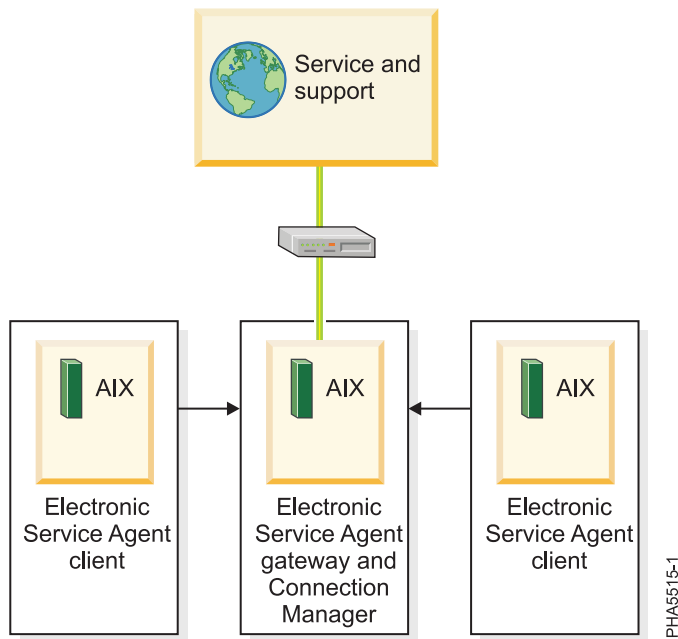


Figure 13. The flow of service information and problems through the service connection from the servers to service and support.

Task 5. Obtain or verify an IBM ID:

If you are using AIX V5R3.J or later or are using Linux, you will need an ID so that you can view information that has been reported to IBM through Electronic Service Agent.

1. Go to the My IBM Profile Web site.
2. Verify that you are registered.
 - If you are registered, Welcome back will be displayed on the Web site. Or, you can select **Sign in** and see if your e-mail address is recognized.
 - If you are not registered, select **Register** and fill out the registration form. Create an IBM ID for each of the people you want to have access to the information that Electronic Service Agent reports to IBM. You must associate these accounts with a server, usually your central server. (You can add other servers later.) The people for whom you create IDs must have system administrator authority on all registered servers.
3. Record your IBM ID (the e-mail address that you registered).
4. Continue with "Task 6. Install the operating system on your server."

Task 6. Install the operating system on your server:

For details, refer to Installing operating systems.

Task 7. Configure your TCP/IP network:

For instructions, refer to the operating system documentation.

Task 8. Activate TCP/IP on your server or logical partitions:

TCP/IP starts automatically, as long as the network adapter is recognized and can communicate with the network when the AIX or Linux operating system is started.

Task 9. Obtain and configure Electronic Service Agent for AIX or Linux:

1. Obtain Electronic Service Agent.
 - a. Go to the Electronic Service Agent Web site.
 - b. Follow the on-screen prompts to locate the instructions to obtain Electronic Service Agent.
2. Choose from the following options:
 - To configure Electronic Service Agent for AIX, continue with the next step.
 - To configure Electronic Service Agent for Linux, go to step 8 on page 34.
3. To configure Electronic Service Agent for AIX, review the following information:

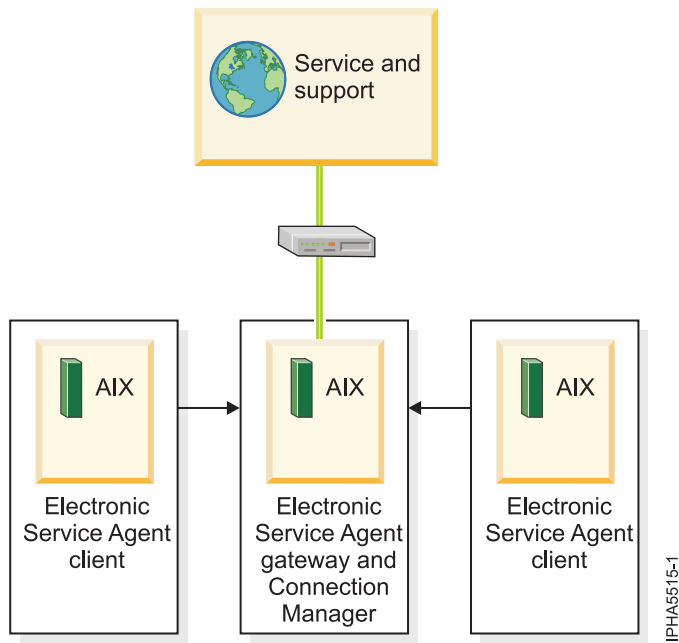
In this example, you will configure the following:

- Electronic Service Agent on the server that has a modem for dial-up connection to service and support

Note: Alternatively, you can use an Internet or Secure Sockets Layer (SSL) connection instead of the modem to connect to service and support.

- Electronic Service Agent on the other clients to communicate with the server that has the modem

Figure 14. This diagram shows three servers and their connection through a modem to service and support.



Note: For complex network environments involving HTTP proxies, SOCKS proxies, or DMZs, refer to the *Electronic Service Agent for IBM pSeries® and IBM RS/6000® User's Guide*.

4. From the System Management Interface Tool (SMIT), configure and start Service Agent Connection Manager (SACM). The SACM is responsible for establishing connectivity to service and support. It enables the gateway server and clients to use a single, secure connection.

Note: More details on SMIT, see System Management Interface Tool SMIT.

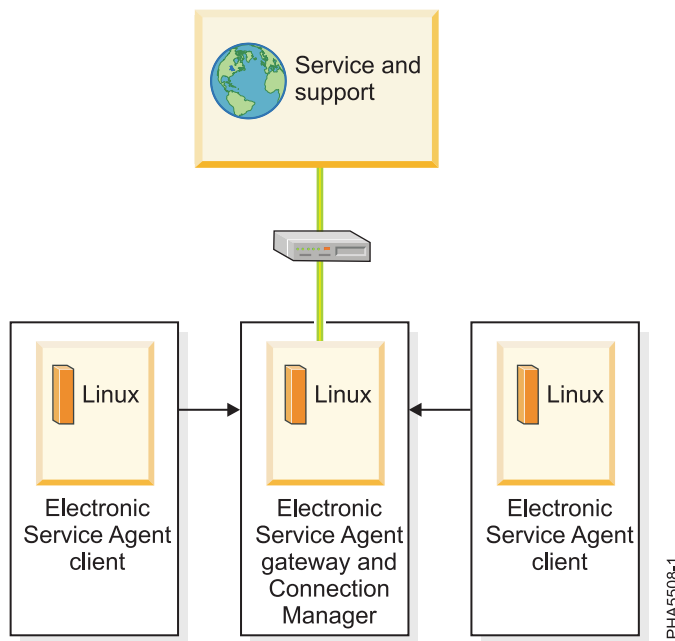
- a. Verify that the host name for the SACM is correct. In this example, the SACM is located on the server or logical partition with the modem. Therefore, the SACM is configured to the host name of the server or logical partition with the modem.
- b. Verify the default port 1198. In most cases, the default port is appropriate. You can change the port later, if necessary. This port is necessary for communication between the gateway server and the SACM.
5. Configure and start the Electronic Service Agent gateway server. This is the server or logical partition that acts as the central management server for all of the clients (monitored servers or logical partitions). The Service Agent gateway server contains the central database, and it initiates communication to service and support. The Service Agent gateway communicates to service and support through the SACM.
 - a. Verify that the host name is correct. In this example, the SACM and SA gateway server are located on the same server. It is the server or logical partition with the modem. 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.
 - b. Verify that the machine type, model, and serial number are correct.
6. Configure and start the Electronic Service Agent client. This is the monitored server or logical partition for which system information is collected and reported to service and support.
 - a. Verify that the host names for the SA clients and for the SA gateway are correct.
 - b. Verify that the machine type, model, and serial number are correct.
7. Continue with "Task 10. Use the Service Agent (SA) Basic User Interface" on page 35.
8. To configure Electronic Service Agent for Linux, review the following information.
In this example, you will configure the following:

- Electronic Service Agent on the server that has a modem for dial-up connection to service and support

Note: Alternatively, you can use an Internet or Secure Sockets Layer (SSL) connection instead of the modem to connect to service and support.

- Electronic Service Agent on the other clients to communicate with the server that has the modem

Figure 15. This diagram shows three servers and their connection through a modem to service and support.



9. From the Linux command line, type the following command to configure and start Service Agent Connection Manager (SACM):

```
startsrc -s sacm
```

The SACM application enables the gateway server and client servers to use a single, secure connection to reach service and support.

10. From the Linux command line, type the following command to configure and start the Electronic Service Agent gateway server:

```
/usr/svcagent/bin/sagatewayconfig
```

The Service Agent gateway server acts as the central management server for all of the clients (monitored servers or logical partitions). It contains the central database and initiates communication to service and support.

11. Continue with "Task 10. Use the Service Agent (SA) Basic User Interface."

Task 10. Use the Service Agent (SA) Basic User Interface:

1. Get familiar with the SA 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.
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 guides you through the appropriate properties. For example, if you specify that you want to use a modem in the Connection Manager 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 or Linux and you use a modem for outbound connectivity, you need to complete specific information for the following properties:

ConnectionManager

Clear **False** for **Connect to SDR using Dialer** to enable the dialer. This indicates that you want to use a modem to connect to service and support.

Dialer Specify details about your modem and service and support connection parameters.

Machines

Add two SA client servers.

Enroll Register the servers with service and support. This initiates a call to service and support to enroll the servers in service and support's database. To complete the process, service and support sends you a key.

Call log

Check the status of the call to service and support. You can see whether the call to service and support is successful.

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.

Task 11. Register the ID with Electronic Service Agent for AIX or Linux:

1. From the Service Agent Basic User Interface, click **Enroll**.
2. Complete the required fields on the right side of the interface. Required fields are indicated with an exclamation point.
3. Continue with "Task 12. Test the connection to service and support."

Task 12. Test the connection to service and support:

1. To test the connection for AIX (if you set up Electronic Service Agent on the server or logical partition), follow these steps:
 - a. From the System Management Interface Tool (SMIT) on your Electronic Service Agent server, activate the Electronic Service Agent.
 - b. Ensure that the Electronic Service Agent Connection Manager is active if it is located on a machine other than the Electronic Service Agent server.
 - c. From SMIT, start the Service Agent Advanced User Interface.
 - d. To use a modem, follow the instructions to configure the dialer on the Connection Manager screen. The default is to connect to service and support using an existing Internet connection.
 - e. Open the **Manual Tools** folder.
 - f. Select **Connect**.
 - g. Monitor the CallLog for the following entry: TEST Connection (Success: 1, Fail: 0).
2. To test the connection for Linux (if you set up Electronic Service Agent on the server or logical partition), follow these steps:
 - a. On your Electronic Service Agent server, activate the Electronic Service Agent.
 - b. At a Linux command line, type the following:
`startsrc -g svcagent`
 - c. Ensure that the Electronic Service Agent Connection Manager is active if it is located on a machine other than the Electronic Service Agent server.
 - d. At a Linux command line, type the following:
`startsrc -s sacm`
 - e. Start the Service Agent Advanced User Interface.
 - f. At a Linux command line, type the following:

/usr/svcagent/bin/sauiascii

- g. If you want to use a modem, follow the instructions to configure the dialer on the Connection Manager screen. The default is to connect to service and support using an existing Internet connection.
- h. Open the **Manual Tools** folder.
- i. Click **Connection**.
- j. Monitor the CallLog for the following entry: TEST Connection (Success: 1, Fail: 0).

Task 13. View the server information that was reported:

You can use the Internet to view details of the system you have enabled, and see the data collected by Electronic Service Agent. To use the advanced features and receive the full benefits of Electronic Service Agent, you must enter an IBM Registration ID (IBM ID). The first IBM ID entered will have Administrator authority and is able to authorize additional users on the Web site. The second IBM ID is available as a backup for the Administrator.

1. Go to the IBM Electronic Services Web site.
2. Click **Sign in** (in the upper-right corner).
3. Type the IBM ID and password.
4. Choose the following options from the navigation bar:
 - To view your server information, click **My systems**.
 - To search technical support using your server information to improve the search results, click **Premium Search**.

Note: In some cases, the Premium Search feature is available only while your server is under warranty or afterward through a service contract.

- To view information related to your servers and interests, click **My messages**.
5. Enter the requested information.

Setting up a clustered environment to connect to service and support

Learn about all the tasks you need to perform to set up connectivity to service and support when you are working in a clustered environment.

Perform or verify Tasks 1 through 16 to set up connectivity for a clustered environment.

Task 1. Before you begin:

This procedure contains the complete list of tasks needed to set up connectivity to service and support. Some of these tasks might already have been completed (during initial server setup, for example). If so, you can use this procedure to verify that the tasks were completed correctly.

In this document, an *Internet connection* is defined as access to the Internet from a logical partition, server, or HMC by direct or indirect access. *Indirect* means that you are behind a Network Address Translation (NAT) firewall. *Direct* means that you have a globally routable address without an intervening firewall, which would block the ports that are needed for communication to service and support.

Task 2. Decide on your connectivity method:

Choose the method that best describes your situation.

If you have an HMC and have multiple logical partitions:

- For the HMC, use one of the following methods:
 - Direct Internet including VPN or a Secure Sockets Layer (SSL) connection
 - Shared direct Internet

- Shared dial-up connection

Note: If you have multiple HMCs on the same subnet, or HMCs that manage common systems, only one HMC needs to connect to service and support. This allows connectivity to be concentrated through one HMC which simplifies firewall rules.

- For AIX or Linux logical partitions, hardware errors will be reported through the HMC, using the connection method provided for the HMC.

If you do not have an HMC and have AIX or Linux:

- If you do not have logical partitions, use one of the following:
 - Internet connection over Secure Sockets Layer (SSL), default configuration
 - Direct or shared (if more than one server) dial-up connection over SSL
- If you have logical partitions and are using the Integrated Virtualization Manager to manage your server, you might want to configure the service processor to contact service and support when the server is not available. For details, refer to “Task 14. Configure the service processor” on page 46.

Note: If you are using the Integrated Virtualization Manager to manage your server, check Service Focal Point for the Integrated Virtualization Manager to see if you need to contact service and support.

Task 3. Prerequisites:

1. For direct Internet connections, contact the network administrator to verify the following:
 - For HMC environments, if you plan on using VPN for transport, ensure that the following ports are open for communication:
 - Protocol UDP ports 500 and 4500 with the following IP addresses: Boulder: 207.25.252.196 and Rochester: 129.42.160.16
 - ESP (protocol 50) with the following IP addresses: Boulder: 207.25.252.196 and Rochester: 129.42.160.16
 - For HMC environments, if you plan on using Secure Sockets Layer for transport and a firewall is in place between the HMC and the Internet, it must allow outgoing TCP/IP connections on port 443 from the HMC to each of the following IP addresses:
 - 129.42.160.48 and 207.25.252.200 (all regions)
 - 129.42.160.49 and 207.25.252.204 (North or South America)
 - 129.42.160.50 and 207.25.252.205 (all other regions)

Note: You need to specify only the IP addresses necessary to set up access that is appropriate for your region.

- For IBM System p5 or IBM eServer p5 servers in a non-HMC environment, choose from the following options:
 - If HTTPS traffic is restricted, ensure that the following port is open for communication: Protocol TCP port 443 with the following IP addresses: 207.25.252.200 and 129.42.160.48
 - If an HTTP proxy is available within your network, then the Service Agent traffic can be routed to it by specifying the Proxy Type as HTTP and Proxy Port as 80.
 - If multiple logical partitions are sharing an Internet connection, you will need the IP addresses or host names created for TCP/IP and for virtual Ethernet.
2. For a dial-up (modem) connection, determine necessary configuration settings, including:
 - Local area code
 - Predial information, such as dialing 9 to dial outside the network
 - Use of commas if delayed dialing is needed
 - Any special telephone line conditions such as pulse (rotary) dialing or no dialtone.

3. Ensure that TCP/IP is set up and configured correctly. If not, contact the network administrator and consult your operating system documentation.

Task 4. Ensure that your physical networking is set up correctly:

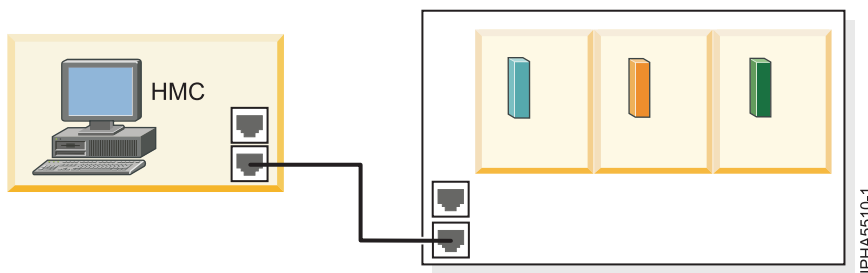
The underlying framework of your service environment is networking. The following networking connections are required for you to be able to take advantage of electronic services such as reporting hardware problems and other server information and downloading updates:

- Between the service processor and the HMC
- Between the HMC and the server (AIX and Linux)
- Between your site and service and support

1. Verify the physical connection between the service processor and the HMC.

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. 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:

Figure 16. This diagram shows the Ethernet connection between your HMC and the service processor on your server.



2. Verify the physical connection between the HMC and the server (AIX and Linux).

This connection allows your server to communicate with your HMC.

How you set up this connection depends on your configuration:

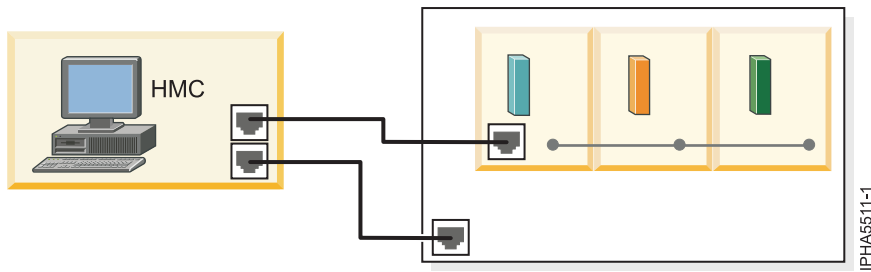
- If your server is in its manufacturing default configuration, you will make this connection when you set up your server.
- If your server has multiple logical partitions, you must ensure that your HMC can communicate with each logical partition and that the logical partitions can communicate with each 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 logical partitions. For instructions on how to configure TCP/IP, see your operating system documentation.

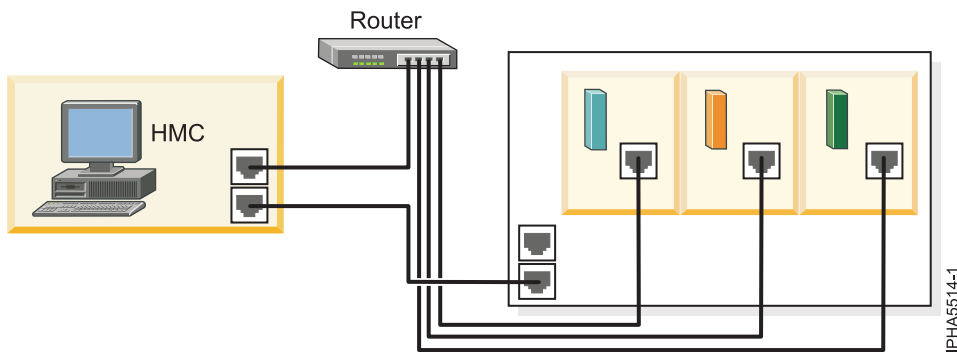
- Have an Ethernet adapter for one logical partition, most likely your service partition, and then use virtual Ethernet to enable the logical partitions to communicate with each other and with the HMC. This option is the preferred option because it requires that you have only one physical adapter in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

Figure 17. This diagram shows the Virtual Ethernet connection between your logical partitions and the physical Ethernet connection between your service partition and the HMC.



- 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:

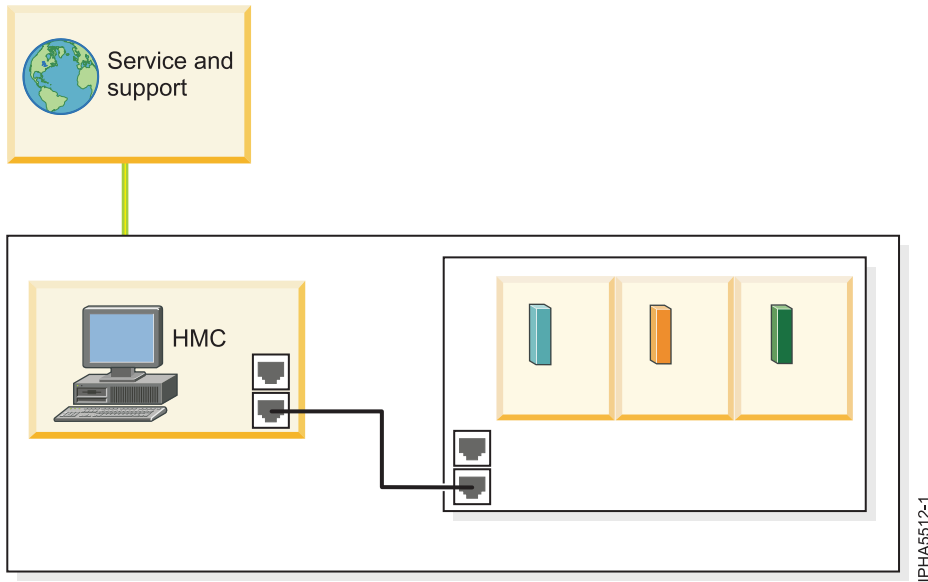
Figure 18. This diagram shows physical Ethernet connections between your logical partitions and your HMC through a router.



3. Verify the physical connection from your site to service and support.

This connection enables you to report hardware problems and other server information to service and support. It also enables you to install updates. This connection is represented in the following illustration:

Figure 19. This diagram shows the connection between service and support and a company that has a server and an HMC.



Task 5. Obtain or verify an IBM ID:

You will need an IBM ID to register IBM Electronic Service Agent on the HMC and for Electronic Service Agent on your operating system or systems. You also will need this ID to view information that has been reported to IBM through Electronic Service Agent.

1. Go to the My IBM Profile Web site.
2. Verify that you are registered.
 - If you are registered, Welcome back will be displayed on the Web site. Or, you can select **Sign in** and see if your e-mail address is recognized.
 - If you are not registered, select **Register** and fill out the registration form. Create an IBM ID for each of the people you want to have access to the information that Electronic Service Agent reports to IBM. You must associate these accounts with a server, usually your central server. (You can add other servers later.) The people for whom you create IDs must have system administrator authority on all registered servers.
3. Record your IBM ID (the e-mail address that you registered).
4. You will need the ID during "Task 6. Verify the HMC service settings using the Guided Setup wizard."

Task 6. Verify the HMC service settings using the Guided Setup wizard:

To verify that the HMC service settings are set up correctly, use the Guided Setup wizard.

Note: If you have not set up your server, do that now. For details, refer to Initial server setup.

1. Access the Guided Setup wizard using the HMC interface:
 - a. In the navigation area, select the HMC that you want to work with.
 - b. Click **Information Center and Setup Wizard**.
 - c. In the contents pane, click **Launch the Guided Setup Wizard**. 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.
2. Click **Next** to skip the tasks that are not specific to setting up service, including:
 - 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
3. Ensure that the following service tasks are completed correctly:

- a. Customer contact information for service-related activities, including:
 - Company name
 - Administrator name
 - E-mail address
 - Telephone numbers
 - Information regarding the location of the HMC
- b. Configuration of connectivity for service-related activities.
 - **Internet VPN**

Note: When configuring the HMC's network settings for connecting using direct or indirect Internet, the HMC must be configured with a default gateway to access the Internet. Select **HMC Management > HMC Configuration > Customize Network Settings**. Ensure that the Default Gateway Information field has a Gateway address listed and a selection is made in the Gateway device field (for example, any).

- **Internet:** Currently, the SSL option must be configured manually:
 - 1) Select **Service Applications → Remote Support → Customize Outbound Connectivity**
 - 2) Select the **Internet** tab.
 - **Dial-up connection from the local HMC**
 - **Connecting through other systems or logical partitions**
- c. Configuration of the network settings.
- For direct or indirect Internet:
 - HMC host name
 - Domain name
 - Description of HMC
 - For a dial-up modem connection:
 - Dial prefix, if applicable
 - Modem configuration, including:
 - Dial type
 - Dial prefix, if applicable
 - Telephone number
- d. Authorize two users for Electronic Service Agent by entering the ID (the e-mail address that you registered with the My Profile Web site at <https://www.ibm.com/account/profile>).

Note: You will be able to authorize more users later.

- e. Add e-mail addresses for those you want to be notified when problem events occur.
4. To test the connection from the HMC, open **Service Applications → Remote Support → Customize Outbound Connectivity**.
5. Select the tab for the type of outbound connectivity that you chose for your HMC (Local Modem, Internet, Internet VPN, or Pass-Through Systems). For more information about these settings, see Choosing your connection method.
6. Click **Test**.
7. Choose from the following options:
- If the test is successful, continue with the next Task.
 - If the test fails, continue with the next step.

8. Ensure that your country or region is listed. Select **Service Applications** → **Remote Support** → **Customize Customer Information**. Ensure that your country or region is selected from the list.
9. Choose from the following options:
 - If you have a dial-up connection, perform the following:
 - Check the telephone line going into the HMC and the wall socket.
 - Check to make sure that you have the telephone number configured correctly, including predial information, such as dialing 9 to dial outside the network.
 - If you have an Internet VPN connection, perform the following:
 - Ensure that the appropriate firewall rules have been added, if necessary.
 - Check that you have a default gateway set up on the HMC. Select **HMC Management** → **HMC Configuration** → **Customize Network Settings**. Ensure that the Default Gateway Information field has a Gateway address listed and a selection is made in the Gateway device field (for example, any).

Task 7. Set up and configure your logical partitions:

For details, refer to Partitioning the server.

Task 8. Install the operating systems on your server or logical partitions:

For details, refer to Installing operating systems.

Task 9. Configure your TCP/IP network:

For instructions, refer to the operating system documentation.

Task 10. Activate TCP/IP on your server or logical partitions:

TCP/IP starts automatically, as long as the network adapter is recognized and can communicate with the network when the AIX or Linux operating system is started.

Task 11. Obtain and configure Electronic Service Agent for AIX or Linux:

If you have an HMC, you do not need to obtain and configure Electronic Service Agent for AIX or Linux. The AIX and Linux inventory and hardware-problem information (or report, perhaps) are sent through the HMC. However, you might want to set up Electronic Service Agent on AIX or Linux to contact the software service organization.

1. Choose from the following options
 - If you have an HMC and do *not* want to obtain and configure Electronic Service Agent for AIX or Linux, continue with “Task 14. Configure the service processor” on page 46.
 - If you want to obtain and configure Electronic Service Agent for AIX or Linux, continue with the next step.
2. Obtain Electronic Service Agent.
 - a. Go to the Electronic Service Agent Web site.
 - b. Follow the on-screen prompts to locate the instructions to obtain Electronic Service Agent.
3. Choose from the following options:
 - To configure Electronic Service Agent for AIX, continue with the next step.
 - To configure Electronic Service Agent for Linux, go to step 9 on page 45.
4. To configure Electronic Service Agent for AIX, review the following information:

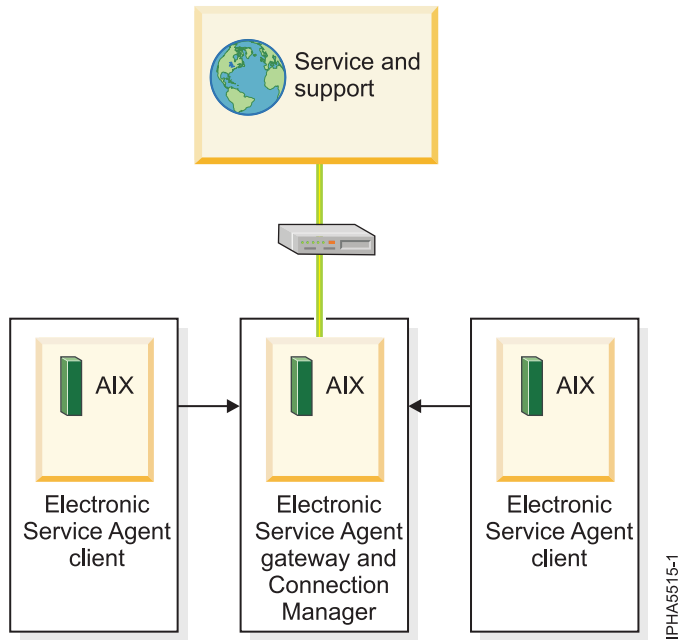
In this example, you will configure the following:

 - Electronic Service Agent on the server that has a modem for dial-up connection to service and support

Note: Alternatively, you can use an Internet or Secure Sockets Layer (SSL) connection instead of the modem to connect to service and support.

- Electronic Service Agent on the other clients to communicate with the server that has the modem

Figure 20. This diagram shows three servers and their connection through a modem to service and support.



Note: For complex network environments involving HTTP proxies, SOCKS proxies, or DMZs, refer to the *Electronic Service Agent for IBM pSeries and IBM RS/6000 User's Guide*.

5. From the System Management Interface Tool (SMIT), configure and start Service Agent Connection Manager (SACM). The SACM is responsible for establishing connectivity to service and support. It enables the gateway server and clients to use a single, secure connection.

Note: More details on SMIT, see System Management Interface Tool SMIT.

- a. Verify that the host name for the SACM is correct. In this example, the SACM is located 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.
 - b. Verify the default port 1198. In most cases, the default port is appropriate. You can change the port later, if necessary. This port is necessary for communication between the gateway server and the SACM.
6. Configure and start the Electronic Service Agent gateway server. This is the server or logical partition that acts as the central management server for all of the clients (monitored servers or logical partitions). The Service Agent gateway server contains the central database, and it initiates communication to service and support. The Service Agent gateway communicates to service and support through the SACM.
 - a. Verify that the host name is correct. In this example, the SACM and SA gateway server are located on the same server. It is the server or logical partition with the modem. 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.
 - b. Verify that the machine type, model, and serial number are correct.
 7. Configure and start the Electronic Service Agent client. This is the monitored server or logical partition for which system information is collected and reported to service and support.

- a. Verify that the host names for the SA clients and for the SA gateway are correct.
- b. Verify that the machine type, model, and serial number are correct.
8. Continue with "Task 12. Use the Service Agent (SA) Basic User Interface."
9. To configure Electronic Service Agent for Linux, review the following information.

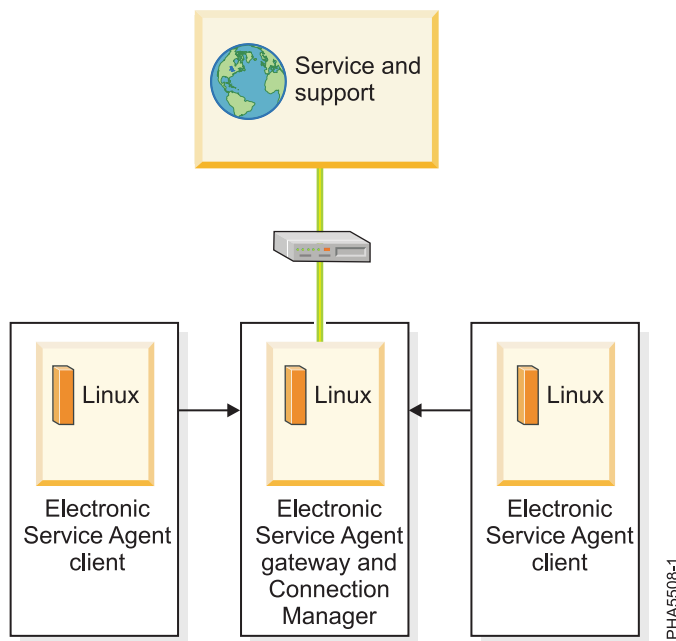
In this example, you will configure the following:

- Electronic Service Agent on the server that has a modem for dial-up connection to service and support

Note: Alternatively, you can use an Internet or Secure Sockets Layer (SSL) connection instead of the modem to connect to service and support.

- Electronic Service Agent on the other clients to communicate with the server that has the modem

Figure 21. This diagram shows three servers and their connection through a modem to service and support.



10. From the Linux command line, type the following command to configure and start Service Agent Connection Manager (SACM):

```
startsrc -s sacm
```

The SACM application enables the gateway server and client servers to use a single, secure connection to reach service and support.

11. From the Linux command line, type the following command to configure and start the Electronic Service Agent gateway server:

```
/usr/svcagent/bin/sagatewayconfig
```

The Service Agent gateway server acts as the central management server for all of the clients (monitored servers or logical partitions). It contains the central database and initiates communication to service and support.

12. Continue with "Task 12. Use the Service Agent (SA) Basic User Interface."

Task 12. Use the Service Agent (SA) Basic User Interface:

You will need to install Electronic Service Agent on AIX or Linux to access the SA Basic User Interface. For details, refer to the Electronic Service Agent Web site and search for the appropriate Electronic Service Agent user's guide.

1. Get familiar with the SA 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.
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 guides you through the appropriate properties. For example, if you specify that you want to use a modem in the Connection Manager 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 or Linux and you use a modem for outbound connectivity, you need to complete specific information for the following properties:

ConnectionManager

Clear **False** for **Connect to SDR using Dialer** to enable the dialer. This indicates that you want to use a modem to connect to service and support.

Dialer Specify details about your modem and service and support connection parameters.

Machines

Add two SA client servers.

Enroll Register the servers with service and support. This initiates a call to service and support to enroll the servers in service and support's database. To complete the process, service and support sends you a key.

Call log

Check the status of the call to service and support. You can see whether the call to service and support is successful.

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.

Task 13. Register the ID with Electronic Service Agent for AIX or Linux:

1. From the Service Agent Basic User Interface, click **Enroll**.
2. Complete the required fields on the right side of the interface. Required fields are indicated with an exclamation point.
3. Continue with "Task 14. Configure the service processor."

Task 14. Configure the service processor:

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 service and support, you need to attach a modem to the system port on your server. In addition, you need to use the Advanced System Management Interface (ASMI) menus to perform several configuration steps.

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.

Note: To perform these tasks, you must have an authority level of either Administrator or Service provider.

2. In the navigation area, expand **System Service Aids**.
3. To configure the service processor system port, follow these steps:
 - a. Select **Serial Port Setup**.

- b. Modify the appropriate fields in the S1 (used with the call-home feature) and S2 (used with the call-in feature) sections.
 - c. Click **Save settings** to save the setting changes.
4. To configure the modem, follow these steps:
 - a. Select **Modem Configuration**.
 - b. Modify the appropriate fields in the S1 and S2 sections.
 - c. Click **Save settings**.
5. To configure the call-home and call-in policy, follow these steps:
 - a. Select **Call-in/Call-home**.
 - b. Enter the desired text into the specified fields.
 - c. Click **Save settings** to save changes.
6. To test the call-home policy, follow these steps:
 - a. Select **Call-Home Test**.
 - b. Click **Initiate call-home test**. A test of the call-home system is performed as specified by the current port and modem selections.
7. Continue with "Task 15. Test the connection to service and support."

Task 15. Test the connection to service and support:

1. If you use an HMC to connect to service and support, follow these steps to test the connection for the HMC:
 - a. On the HMC, open **Service Applications > Service Focal Point > Service Utilities**.
 - b. Select a system.
 - c. Select **Selected > Create serviceable event**.
 - d. Select **Test automatic problem reporting**.
 - e. Select **Request Service**. A message is displayed when the service request is sent.
2. To test the connection for AIX (if you set up Electronic Service Agent on the server or logical partition), follow these steps:
 - a. From the System Management Interface Tool (SMIT) on your Electronic Service Agent server, activate the Electronic Service Agent.
 - b. Ensure that the Electronic Service Agent Connection Manager is active if it is located on a machine other than the Electronic Service Agent server.
 - c. From SMIT, start the Service Agent Advanced User Interface.
 - d. To use a modem, follow the instructions to configure the dialer on the Connection Manager screen. The default is to connect to service and support using an existing Internet connection.
 - e. Open the **Manual Tools** folder.
 - f. Select **Connect**.
 - g. Monitor the CallLog for the following entry: TEST Connection (Success: 1, Fail: 0).
3. To test the connection for Linux (if you set up Electronic Service Agent on the server or logical partition), follow these steps:
 - a. On your Electronic Service Agent server, activate the Electronic Service Agent.
 - b. At a Linux command line, type the following:
`startsrc -g svcagent`
 - c. Ensure that the Electronic Service Agent Connection Manager is active if it is located on a machine other than the Electronic Service Agent server.
 - d. At a Linux command line, type the following:
`startsrc -s sacm`
 - e. Start the Service Agent Advanced User Interface.

- f. At a Linux command line, type the following:
`/usr/svcagent/bin/sauiascii`
- g. If you want to use a modem, follow the instructions to configure the dialer on the Connection Manager screen. The default is to connect to service and support using an existing Internet connection.
- h. Open the **Manual Tools** folder.
- i. Click **Connection**.
- j. Monitor the CallLog for the following entry: TEST Connection (Success: 1, Fail: 0).

Task 16. View the server information that was reported:

You can use the Internet to view details of the system you have enabled, and see the data collected by Electronic Service Agent. To use the advanced features and receive the full benefits of Electronic Service Agent, you must enter an IBM Registration ID (IBM ID). The first IBM ID entered will have Administrator authority and is able to authorize additional users on the Web site. The second IBM ID is available as a backup for the Administrator.

1. Go to the IBM Electronic Services Web site.
2. Click **Sign in** (in the upper-right corner).
3. Type the IBM ID and password.
4. Choose the following options from the navigation bar:
 - To view your server information, click **My systems**.
 - To search technical support using your server information to improve the search results, click **Premium Search**.

Note: In some cases, the Premium Search feature is available only while your server is under warranty or afterward through a service contract.

- To view information related to your servers and interests, click **My messages**.
5. Enter the requested information.

Setting up AIX or Linux to use an HMC to connect to service and support

Learn how to create a service connection to send service information from AIX or Linux logical partitions and servers using an HMC.

Perform or verify Tasks 1 through 16 to set up connectivity for an AIX or Linux logical partitions or servers using an HMC.

Task 1. Before you begin:

This procedure contains the complete list of tasks needed to set up connectivity to service and support. Some of these tasks might already have been completed (during initial server setup, for example). If so, you can use this procedure to verify that the tasks were completed correctly.

In this document, an *Internet connection* is defined as access to the Internet from a logical partition, server, or HMC by direct or indirect access. *Indirect* means that you are behind a Network Address Translation (NAT) firewall. *Direct* means that you have a globally routable address without an intervening firewall, which would block the ports that are needed for communication to service and support.

Task 2. Decide on your connectivity method:

Choose the method that best describes your situation.

If you have an HMC and have multiple logical partitions:

- For the HMC, use one of the following methods:

- Direct Internet including VPN or a Secure Sockets Layer (SSL) connection
- Shared direct Internet
- Shared dial-up connection

Note: If you have multiple HMCs on the same subnet, or HMCs that manage common systems, only one HMC needs to connect to service and support. This allows connectivity to be concentrated through one HMC which simplifies firewall rules.

- For AIX or Linux logical partitions, hardware errors will be reported through the HMC, using the connection method provided for the HMC.

Task 3. Prerequisites:

1. For direct Internet connections, contact the network administrator to verify the following:
 - For HMC environments, if you plan on using VPN for transport, ensure that the following ports are open for communication:
 - Protocol UDP ports 500 and 4500 with the following IP addresses: Boulder: 207.25.252.196 and Rochester: 129.42.160.16
 - ESP (protocol 50) with the following IP addresses: Boulder: 207.25.252.196 and Rochester: 129.42.160.16
 - For HMC environments, if you plan on using Secure Sockets Layer for transport and a firewall is in place between the HMC and the Internet, it must allow outgoing TCP/IP connections on port 443 from the HMC to each of the following IP addresses:
 - 129.42.160.48 and 207.25.252.200 (all regions)
 - 129.42.160.49 and 207.25.252.204 (North or South America)
 - 129.42.160.50 and 207.25.252.205 (all other regions)

Note: You need to specify only the IP addresses necessary to set up access that is appropriate for your region.

- For IBM System p5 or IBM eServer p5 servers in a non-HMC environment, choose from the following options:
 - If HTTPS traffic is restricted, ensure that the following port is open for communication: Protocol TCP port 443 with the following IP addresses: 207.25.252.200 and 129.42.160.48
 - If an HTTP proxy is available within your network, then the Service Agent traffic can be routed to it by specifying the Proxy Type as HTTP and Proxy Port as 80.
 - If multiple logical partitions are sharing an Internet connection, you will need the IP addresses or host names created for TCP/IP and for virtual Ethernet.
2. For a dial-up (modem) connection, determine necessary configuration settings, including:
 - Local area code
 - Predial information, such as dialing 9 to dial outside the network
 - Use of commas if delayed dialing is needed
 - Any special telephone line conditions such as pulse (rotary) dialing or no dialtone.
 3. Ensure that TCP/IP is set up and configured correctly. If not, contact the network administrator and consult your operating system documentation.

Task 4. Ensure that your physical networking is set up correctly:

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 updates:

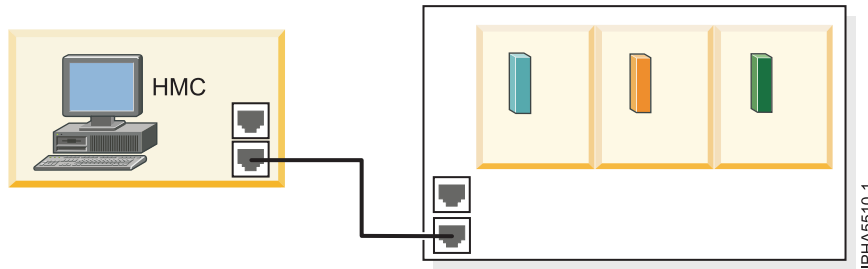
- Between the service processor and the HMC
- Between the HMC and the server (AIX and Linux)

- Between your site and service and support

1. Verify the physical connection between the service processor and the HMC.

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. 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:

Figure 22. This diagram shows the Ethernet connection between your HMC and the service processor on your server.



2. Verify the physical connection between the HMC and the server (AIX and Linux).

This connection allows your server to communicate with your HMC.

How you set up this connection depends on your configuration:

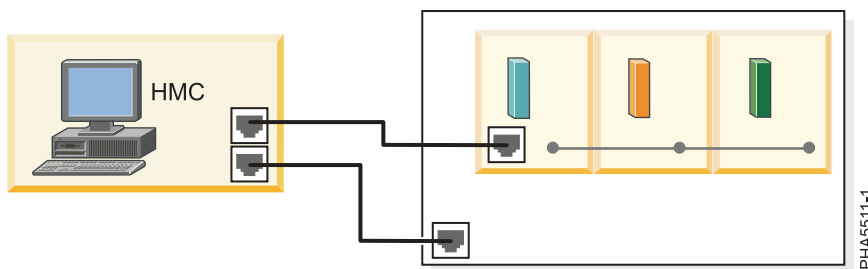
- If your server is in its manufacturing default configuration, you will make this connection when you set up your server.
- If your server has multiple logical partitions, you must ensure that your HMC can communicate with each logical partition and that the logical partitions can communicate with each 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 logical partitions. For instructions on how to configure TCP/IP, see your operating system documentation.

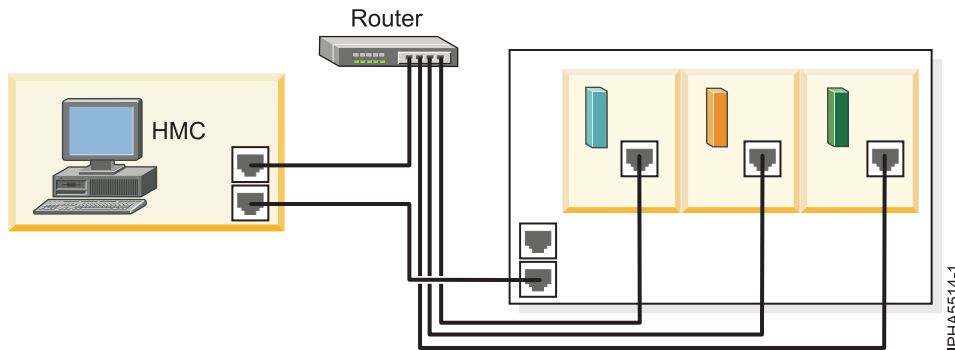
- Have an Ethernet adapter for one logical partition, most likely your service partition, and then use virtual Ethernet to enable the logical partitions to communicate with each other and with the HMC. This option is the preferred option because it requires that you have only one physical adapter in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

Figure 23. This diagram shows the Virtual Ethernet connection between your logical partitions and the physical Ethernet connection between your service partition and the HMC.



- 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:

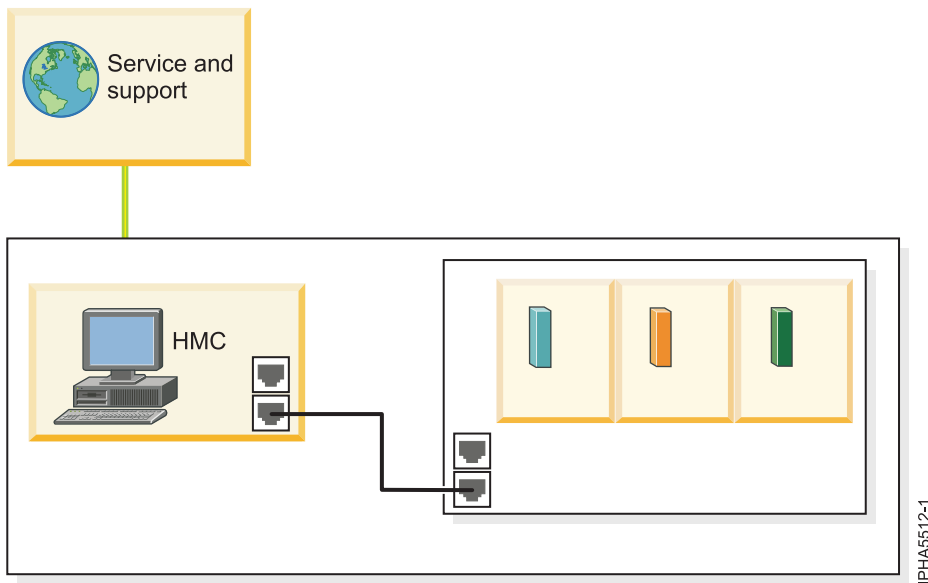
Figure 24. This diagram shows physical Ethernet connections between your logical partitions and your HMC through a router.



3. Verify the physical connection from your site to service and support.

This connection enables you to report hardware problems and other server information to service and support. It also enables you to install updates. This connection is represented in the following illustration:

Figure 25. This diagram shows the connection between service and support and a company that has a server and an HMC.



Task 5. Obtain or verify an IBM ID:

You will need an IBM ID to register IBM Electronic Service Agent on the HMC and for Electronic Service Agent on your operating system or systems. You also will need this ID to view information that has been reported to IBM through Electronic Service Agent.

1. Go to the My IBM Profile Web site.
2. Verify that you are registered.

- If you are registered, Welcome back will be displayed on the Web site. Or, you can select **Sign in** and see if your e-mail address is recognized.
 - If you are not registered, select **Register** and fill out the registration form. Create an IBM ID for each of the people you want to have access to the information that Electronic Service Agent reports to IBM. You must associate these accounts with a server, usually your central server. (You can add other servers later.) The people for whom you create IDs must have system administrator authority on all registered servers.
3. Record your IBM ID (the e-mail address that you registered).
 4. You will need the ID during “Task 6. Verify the HMC service settings.”

Related information

 [My IBM Profile Web site](#)

Task 6. Verify the HMC service settings:

To verify that the HMC service settings are set up correctly, use the Guided Setup wizard.

Note: If you have not set up your server, do that now. For details, refer to Initial server setup.

1. Access the Guided Setup wizard using the HMC interface:
 - a. In the navigation area, select the HMC that you want to work with.
 - b. Click **Information Center and Setup Wizard**.
 - c. In the contents pane, click **Launch the Guided Setup Wizard**. 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.
2. Click **Next** to skip the tasks that are not specific to setting up service, including:
 - 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
3. Ensure that the following service tasks are completed correctly:
 - a. Customer contact information for service-related activities, including:
 - Company name
 - Administrator name
 - E-mail address
 - Telephone numbers
 - Information regarding the location of the HMC
 - b. Configuration of connectivity for service-related activities.
 - **Internet VPN**

Note: When configuring the HMC’s network settings for connecting using direct or indirect Internet, the HMC must be configured with a default gateway to access the Internet. Select **HMC Management > HMC Configuration > Customize Network Settings**. Ensure that the Default Gateway Information field has a Gateway address listed and a selection is made in the Gateway device field (for example, any).

- **Internet:** Currently, the SSL option must be configured manually:
 - 1) Select **Service Applications → Remote Support → Customize Outbound Connectivity**
 - 2) Select the **Internet** tab.
- **Dial-up connection from the local HMC**
- **Connecting through other systems or logical partitions**

- c. Configuration of the network settings.
 - For direct or indirect Internet:
 - HMC host name
 - Domain name
 - Description of HMC
 - For a dial-up modem connection:
 - Dial prefix, if applicable
 - Modem configuration, including:
 - Dial type
 - Dial prefix, if applicable
 - Telephone number
- d. Authorize two users for Electronic Service Agent by entering the ID (the e-mail address that you registered with the My Profile Web site at <https://www.ibm.com/account/profile>).

Note: You will be able to authorize more users later.

- e. Add e-mail addresses for those you want to be notified when problem events occur.
4. To test the connection from the HMC, open **Service Applications** → **Remote Support** → **Customize Outbound Connectivity**.
 5. Select the tab for the type of outbound connectivity that you chose for your HMC (Local Modem, Internet, Internet VPN, or Pass-Through Systems). For more information about these settings, see *Choosing your connection method*.
 6. Click **Test**.
 7. Choose from the following options:
 - If the test is successful, continue with the next Task.
 - If the test fails, continue with the next step.
 8. Ensure that your country or region is listed. Select **Service Applications** → **Remote Support** → **Customize Customer Information**. Ensure that your country or region is selected from the list.
 9. Choose from the following options:
 - If you have a dial-up connection, perform the following:
 - Check the telephone line going into the HMC and the wall socket.
 - Check to make sure that you have the telephone number configured correctly, including predial information, such as dialing 9 to dial outside the network.
 - If you have an Internet VPN connection, perform the following:
 - Ensure that the appropriate firewall rules have been added, if necessary.
 - Check that you have a default gateway set up on the HMC. Select **HMC Management** → **HMC Configuration** → **Customize Network Settings**. Ensure that the Default Gateway Information field has a Gateway address listed and a selection is made in the Gateway device field (for example, any).

Related concepts

“Choosing your connection method” on page 4
Learn about choosing your connection method.

Related information

Initial server setup

Task 7. Set up and configure your logical partitions:

For details, refer to *Partitioning the server*.

Related information

Partitioning the server

Task 8. Install the operating systems on your server or logical partitions:

For details, refer to Installing operating systems.

Related information

Installing operating systems

Task 9. Configure your TCP/IP network:

For instructions, refer to the operating system documentation.

Task 10. Activate TCP/IP on your server or logical partitions:

TCP/IP starts automatically, as long as the network adapter is recognized and can communicate with the network when the AIX or Linux operating system is started.

Task 11. Obtain and configure Electronic Service Agent for AIX or Linux:

If you have an HMC, you do not need to obtain and configure Electronic Service Agent for AIX or Linux. The AIX and Linux inventory and hardware-problem information (or report, perhaps) are sent through the HMC. However, you might want to set up Electronic Service Agent on AIX or Linux to contact the software service organization.

1. Choose from the following options:
 - If you have an HMC and do *not* want to obtain and configure Electronic Service Agent, continue with “Task 14. Configure the service processor” on page 57.
 - If you want to obtain and configure Electronic Service Agent for AIX or Linux, continue with the next step.
2. Obtain Electronic Service Agent.
 - a. Go to the Electronic Service Agent Web site.
 - b. Follow the on-screen prompts to locate the instructions to obtain Electronic Service Agent.
3. Choose from the following options:
 - To configure Electronic Service Agent AIX, continue with the next step.
 - To configure Electronic Service Agent for Linux, go to step 9 on page 55.
4. To configure Electronic Service Agent for AIX, review the following information:

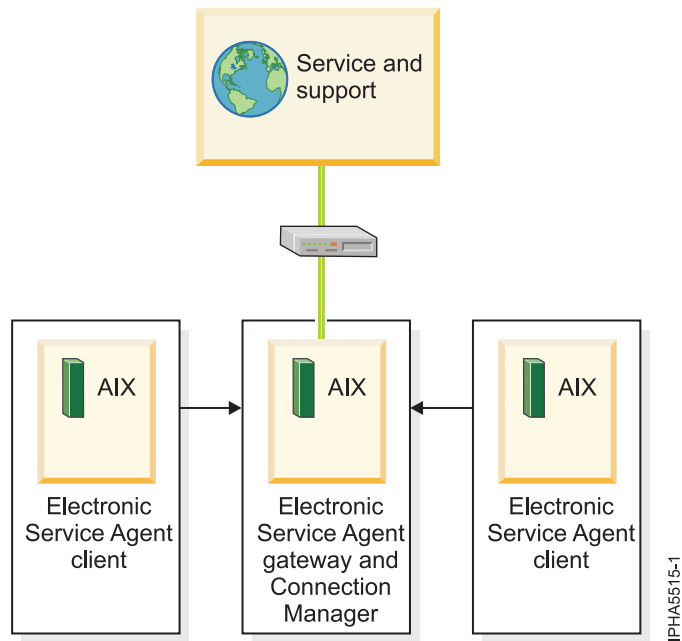
In this example, you will configure the following:

 - Electronic Service Agent on the server that has a modem for dial-up connection to service and support

Note: Alternatively, you can use an Internet or Secure Sockets Layer (SSL) connection instead of the modem to connect to service and support.

 - Electronic Service Agent on the other clients to communicate with the server that has the modem

Figure 26. This diagram shows three servers and their connection through a modem to service and support.



Note: For complex network environments involving HTTP proxies, SOCKS proxies, or DMZs, refer to the *Electronic Service Agent for IBM pSeries and IBM RS/6000 User's Guide*.

5. From the System Management Interface Tool (SMIT), configure and start Service Agent Connection Manager (SACM). The SACM is responsible for establishing connectivity to service and support. It enables the gateway server and clients to use a single, secure connection.

Note: For more details on SMIT, see the System Management Interface Tool SMIT Redbook.

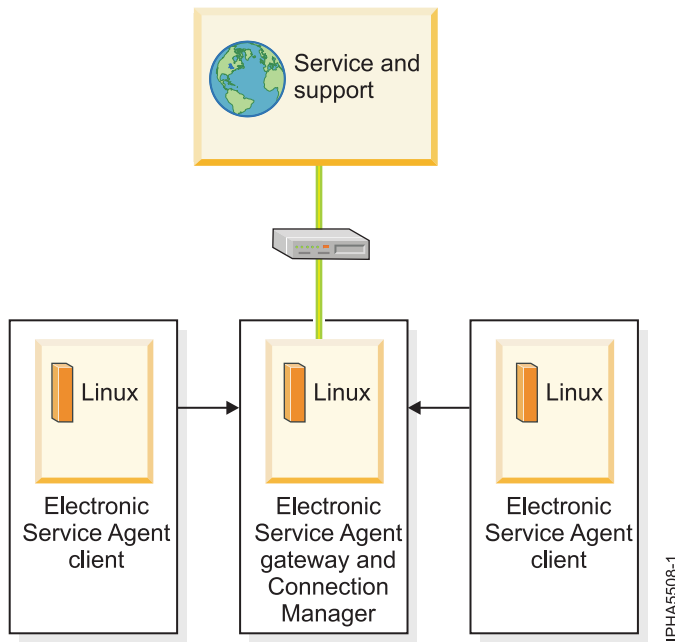
- a. Verify that the host name for the SACM is correct. In this example, the SACM is located on the server or logical partition with the modem. Therefore, the SACM is configured to the host name of the server or logical partition with the modem.
- b. Verify the default port 1198. In most cases, the default port is appropriate. You can change the port later, if necessary. This port is necessary for communication between the gateway server and the SACM.
6. Configure and start the Electronic Service Agent gateway server. This is the server or logical partition that acts as the central management server for all of the clients (monitored servers or logical partitions). The Service Agent gateway server contains the central database, and it initiates communication to service and support. The Service Agent gateway communicates to service and support through the SACM.
 - a. Verify that the host name is correct. In this example, the SACM and SA gateway server are located on the same server. It is the server or logical partition with the modem. 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.
 - b. Verify that the machine type, model, and serial number are correct.
7. Configure and start the Electronic Service Agent client. This is the monitored server or logical partition for which system information is collected and reported to service and support.
 - a. Verify that the host names for the SA clients and for the SA gateway are correct.
 - b. Verify that the machine type, model, and serial number are correct.
8. Continue with "Task 12. Use the Service Agent (SA) Basic User Interface" on page 56.
9. To configure Electronic Service Agent for Linux, review the following information.
In this example, you will configure the following:

- Electronic Service Agent on the server that has a modem for dial-up connection to service and support

Note: Alternatively, you can use an Internet or Secure Sockets Layer (SSL) connection instead of the modem to connect to service and support.

- Electronic Service Agent on the other clients to communicate with the server that has the modem

Figure 27. This diagram shows three servers and their connection through a modem to service and support.



- From the Linux command line, type the following command to configure and start Service Agent Connection Manager (SACM):

```
startsrc -s sacm
```

The SACM application enables the gateway server and client servers to use a single, secure connection to reach service and support.

- From the Linux command line, type the following command to configure and start the Electronic Service Agent gateway server:

```
/usr/svcagent/bin/sagatewayconfig
```

The Service Agent gateway server acts as the central management server for all of the clients (monitored servers or logical partitions). It contains the central database and initiates communication to service and support.

- Continue with "Task 12. Use the Service Agent (SA) Basic User Interface."

Related information

- ➡ Electronic Service Agent Web site
- ➡ System Management Interface Tool SMIT

Task 12. Use the Service Agent (SA) Basic User Interface:

You will need to install Electronic Service Agent on AIX or Linux to access the SA Basic User Interface. For details, refer to the Electronic Service Agent Web site and search for the appropriate Electronic Service Agent user's guide.

1. Get familiar with the SA 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.
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 guides you through the appropriate properties. For example, if you specify that you want to use a modem in the Connection Manager 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 or Linux and you use a modem for outbound connectivity, you need to complete specific information for the following properties:

ConnectionManager

Clear **False** for **Connect to SDR using Dialer** to enable the dialer. This indicates that you want to use a modem to connect to service and support.

Dialer Specify details about your modem and service and support connection parameters.

Machines

Add two SA client servers.

Enroll Register the servers with service and support. This initiates a call to service and support to enroll the servers in service and support's database. To complete the process, service and support sends you a key.

Call log

Check the status of the call to service and support. You can see whether the call to service and support is successful.

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.

Related information

 [Electronic Service Agent Web site](#)

Task 13. Register the ID with Electronic Service Agent for AIX or Linux:

1. From the Service Agent Basic User Interface, click **Enroll**.
2. Complete the required fields on the right side of the interface. Required fields are indicated with an exclamation point.
3. Continue with "Task 14. Configure the service processor."

Task 14. Configure the service processor:

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 service and support, you need to attach a modem to the system port on your server. In addition, you need to use the Advanced System Management Interface (ASMI) menus to perform several configuration steps.

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.

Note: To perform these tasks, you must have an authority level of either Administrator or Service provider.

2. In the navigation area, expand **System Service Aids**.
3. To configure the service processor system port, follow these steps:
 - a. Select **Serial Port Setup**.

- b. Modify the appropriate fields in the S1 (used with the call-home feature) and S2 (used with the call-in feature) sections.
 - c. Click **Save settings** to save the setting changes.
4. To configure the modem, follow these steps:
 - a. Select **Modem Configuration**.
 - b. Modify the appropriate fields in the S1 and S2 sections.
 - c. Click **Save settings**.
5. To configure the call-home and call-in policy, follow these steps:
 - a. Select **Call-in/Call-home**.
 - b. Enter the desired text into the specified fields.
 - c. Click **Save settings** to save changes.
6. To test the call-home policy, follow these steps:
 - a. Select **Call-Home Test**.
 - b. Click **Initiate call-home test**. A test of the call-home system is performed as specified by the current port and modem selections.
7. Continue with "Task 15. Test the connection to service and support."

Task 15. Test the connection to service and support:

1. If you use an HMC to connect to service and support, follow these steps to test the connection for the HMC:
 - a. On the HMC, open **Service Applications > Service Focal Point > Service Utilities**.
 - b. Select a system.
 - c. Select **Selected > Create serviceable event**.
 - d. Select **Test automatic problem reporting**.
 - e. Select **Request Service**. A message is displayed when the service request is sent.
2. To test the connection for AIX (if you set up Electronic Service Agent on the server or logical partition), follow these steps:
 - a. From the System Management Interface Tool (SMIT) on your Electronic Service Agent server, activate the Electronic Service Agent.
 - b. Ensure that the Electronic Service Agent Connection Manager is active if it is located on a machine other than the Electronic Service Agent server.
 - c. From SMIT, start the Service Agent Advanced User Interface.
 - d. To use a modem, follow the instructions to configure the dialer on the Connection Manager screen. The default is to connect to service and support using an existing Internet connection.
 - e. Open the **Manual Tools** folder.
 - f. Select **Connect**.
 - g. Monitor the CallLog for the following entry: TEST Connection (Success: 1, Fail: 0).
3. To test the connection for Linux (if you set up Electronic Service Agent on the server or logical partition), follow these steps:
 - a. On your Electronic Service Agent server, activate the Electronic Service Agent.
 - b. At a Linux command line, type the following:
startsrc -g svcagent
 - c. Ensure that the Electronic Service Agent Connection Manager is active if it is located on a machine other than the Electronic Service Agent server.
 - d. At a Linux command line, type the following:
startsrc -s sacm
 - e. Start the Service Agent Advanced User Interface.

- f. At a Linux command line, type the following:
`/usr/svcagent/bin/sauiascii`
- g. If you want to use a modem, follow the instructions to configure the dialer on the Connection Manager screen. The default is to connect to service and support using an existing Internet connection.
- h. Open the **Manual Tools** folder.
- i. Click **Connection**.
- j. Monitor the CallLog for the following entry: TEST Connection (Success: 1, Fail: 0).

Task 16. View the server information that was reported:

You can use the Internet to view details of the system you have enabled, and see the data collected by Electronic Service Agent. To use the advanced features and receive the full benefits of Electronic Service Agent, you must enter an IBM Registration ID (IBM ID). The first IBM ID entered will have Administrator authority and is able to authorize additional users on the Web site. The second IBM ID is available as a backup for the Administrator.

1. Go to the Electronic Service Agent Web site.
 2. Click **Sign in** (in the upper-right corner).
 3. Type the IBM ID and password.
 4. Choose the following options from the navigation bar:
 - To view your server information, click **My systems**.
 - To search technical support using your server information to improve the search results, click **Premium Search**.
- Note:** In some cases, the Premium Search feature is available only while your server is under warranty or afterward through a service contract.
- To view information related to your servers and interests, click **My messages**.
 5. Enter the requested information.

Related information

 [Electronic Service Agent Web site](#)

Setting up AIX or Linux to connect to service and support without an HMC

Learn how to create a service connection to send service information from AIX or Linux servers to service and support.

Perform or verify Tasks 1 through 14 to set up connectivity for an AIX or Linux server or servers.

Task 1. Before you begin:

This procedure contains the complete list of tasks needed to set up connectivity to service and support.

In this document, an *Internet connection* is defined as access to the Internet from a logical partition or server by direct or indirect access. *Indirect* means that you are behind a Network Address Translation (NAT) firewall. *Direct* means that you have a globally routable address without an intervening firewall, which would block the ports that are needed for communication to service and support.

Task 2. Decide on your connectivity method:

Choose the method that best describes your situation.

- If you do not have logical partitions, use one of the following:
 - Internet connection over Secure Sockets Layer (SSL), default configuration
 - Direct or shared (if more than one server) dial-up connection over SSL

- If you have logical partitions and are using the Integrated Virtualization Manager to manage your server, you might want to configure the service processor to contact service and support when the server is not available. For details, refer to “Task 12. Configure the service processor” on page 64.

Note: If you are using the Integrated Virtualization Manager to manage your server, check Service Focal Point for the Integrated Virtualization Manager to see if you need to contact service and support.

Task 3. Prerequisites:

Depending on your situation, complete one of the following:

- For IBM System p5 or IBM eServer p5 servers, choose from the following options:
 - If an HTTP proxy is available within your network, then the Service Agent traffic can be routed to it by specifying the Proxy Type as HTTP and Proxy Port as 80.
 - If HTTPS traffic is restricted, ensure that the following port is open for communication: Protocol TCP port 443 with the following IP addresses: 207.25.252.200 and 129.42.160.48
- For dial-up (modem) connection, determine necessary configuration settings, including:
 - Local area code
 - Predial information, such as dialing 9 to dial outside the network
 - Use of commas if delayed dialing is needed
 - Point to Point Protocol (PPP) required for dial connection
 - Available tty or vty devices

Task 4. Ensure that your physical network is set up correctly:

Verify the physical connection from your site to service and support. This connection enables you to report hardware problems and other server information to service and support. It also enables you to install updates. This connection is represented in the following illustration:

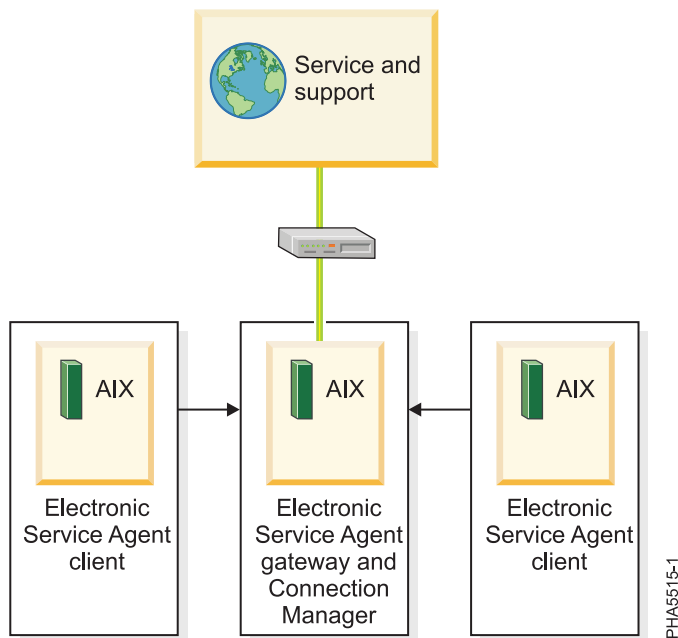


Figure 28. The flow of service information and problems through the service connection from the servers to service and support.

Task 5. Obtain or verify an ID:

If you are using AIX V5R3 or earlier or are using Linux, you will need an IBM ID to register IBM Electronic Service Agent for AIX and Linux. You will also need this ID to view information that has been reported to IBM through Electronic Service Agent.

If you are using AIX V5R3.J or later or are using Linux, you will need an ID so that you can view information that has been reported to IBM through Electronic Service Agent.

1. Go to the My IBM Profile Web site.
2. Verify that you are registered.
 - If you are registered, Welcome back will be displayed on the Web site. Or, you can select **Sign in** and see if your e-mail address is recognized.
 - If you are not registered, select **Register** and fill out the registration form. Create an IBM ID for each of the people you want to have access to the information that Electronic Service Agent reports to IBM. You must associate these accounts with a server, usually your central server. (You can add other servers later.) The people for whom you create IDs must have system administrator authority on all registered servers.
3. Record your IBM ID (the e-mail address that you registered).

Important: To ensure your registered hosts are assigned to your ID, you will need to enter your IBM ID in the Network data field in "Task 10. Use the Service Agent (SA) Basic User Interface".

Related information

 My IBM Profile Web site

Task 6. Install the operating system on your server:

For details, refer to Installing operating systems.

Related information

Installing operating systems

Task 7. Configure your TCP/IP network:

For instructions, refer to the operating system documentation.

Task 8. Activate TCP/IP on your server:

TCP/IP starts automatically, as long as the network adapter is recognized and can communicate with the network when the AIX or Linux operating system is started.

Task 9. Obtain and configure Electronic Service Agent for AIX or Linux:

1. Obtain Electronic Service Agent. If you are using AIX V5R3 or earlier or are using Linux, go to the Electronic Service Agent Web site and follow the on-screen prompts to locate the instructions to obtain Electronic Service Agent. If you are using AIX V5R3.J or later or are using Linux, Electronic Service Agent is available on the AIX V5R3.J installation media or on the Electronic Service Agent Web site.
2. Install the selected code and any prerequisites that you obtained in the previous step.
3. Choose from the following options:
 - To configure Electronic Service Agent for AIX, continue with the next step.
 - To configure Electronic Service Agent for Linux, go to step 10 on page 63.
4. To configure Electronic Service Agent for AIX, review the following information:

In this example, you will configure Electronic Service Agent on the server that has a modem for dial-up connection to service and support.

Note: Alternatively, you can use an Internet connection instead of the modem to connect to service and support.

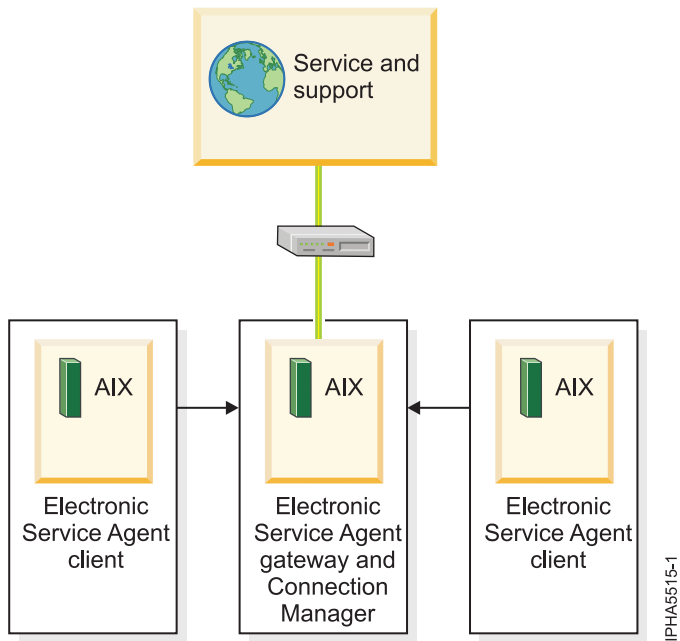


Figure 29. This diagram shows two AIX Service Agent clients attached to one AIX Service Agent gateway that is attached to a modem to access service and support.

Note: For complex network environments involving HTTP proxies, SOCKS proxies, or DMZs, refer to the *Electronic Service Agent for IBM pSeries and IBM RS/6000 User's Guide*.

5. From the System Management Interface Tool (SMIT), configure and start Service Agent Connection Manager (SACM). The SACM is responsible for establishing connectivity to service and support. It enables the master or slave gateway server to use a single, secure connection.

Note: More details on SMIT, see System Management Interface Tool SMIT at <http://www.redbooks.ibm.com/abstracts/redp0105.html>.

- a. In this example, the SACM is located on the server or logical partition with the modem. The SACM default configuration of hostname *blank* or *localhost*, port *1198*, and secure setting should be verified.
- b. If configuration is altered from the default configuration, the Call Controller template on the master SA gateway must have corrected information entered in field "URL2CM". If this information is not correct, the call log will report the following, A remote host refused an attempted connect operation.
6. Configure and start the Electronic Service Agent gateway server. This is the server or logical partition that acts as the central management server for all of the clients (monitored servers or logical partitions). The Service Agent gateway server contains the central database, and it initiates communication to service and support. The Service Agent gateway communicates to service and support through the SACM.
 - a. In this example, the SACM and SA gateway servers are located on the same server. 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.
 - b. Verify that the machine type, model, and serial number are correct.
7. Ensure that the AIX Electronic Service Agent common gateway database has been started and initialized. The client host can be configured and started in two ways.

- By installing the client image from the installation media and using the **Manage SA Client** option in SMIT to configure the client host locally.
 - From the Gateway SA user interface (Machines tab).
8. Configure and start the Electronic Service Agent client. This is the monitored server or logical partition for which system information is collected and reported to service and support.
 - a. Verify that the host names for the SA clients and for the SA gateway are correct.
 - b. Verify that the machine type, model, and serial number are correct.
 - c. Enter the password to match the SA gateway user interface password.
 9. Continue with "Task 10. Use the Service Agent (SA) Basic User Interface" on page 64.
 10. To configure Electronic Service Agent for Linux, review the following information.
In this example, you will configure Electronic Service Agent on the server that has a modem for dial-up connection to service and support

Note: Alternatively, you can use an Internet connection instead of the modem to connect to service and support.

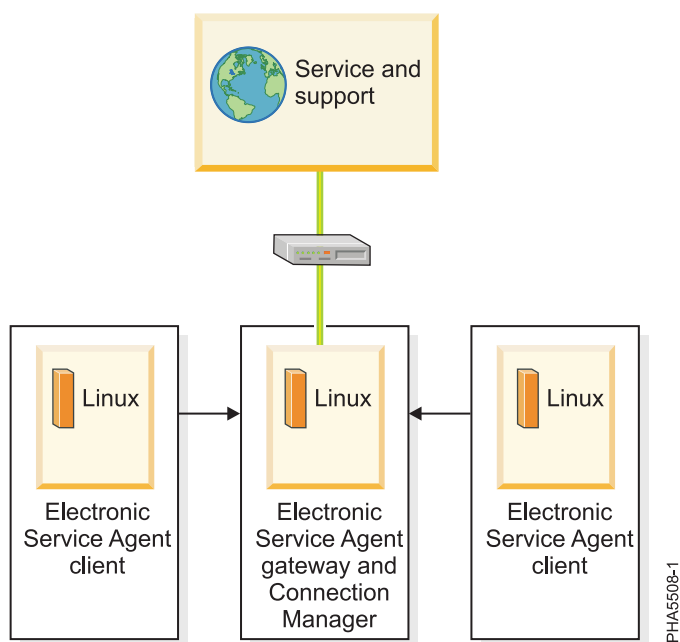


Figure 30. This diagram shows two Service Agent clients attached to one Service Agent gateway that is attached to a modem to access service and support.

11. From the Linux command prompt, type the following command to configure and start Service Agent Connection Manager (SACM):


```
startsrc -s sacm
```

The SACM application enables the gateway server and client servers to use a single, secure connection to reach service and support.
12. From the Linux command prompt, type the following command to configure and start the Electronic Service Agent gateway server:

```
/usr/svcagent/bin/sagatewayconfig
```

The Service Agent gateway server acts as the central management server for all of the clients (monitored servers or logical partitions). It contains the central database and initiates communication to service and support.

Related information

-  [Electronic Service Agent Web site](#)
-  [System Management Interface Tool SMIT](#)

Task 10. Use the Service Agent (SA) Basic User Interface:

1. Get familiar with the SA 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.
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 guides you through the appropriate properties. For example, if you specify that you want to use a modem in the Connection Manager 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 or Linux and you use a modem for outbound connectivity, you need to complete specific information for the following properties:

CallController

Verify URL2CM is the default `https://localhost:1198`. Or correct to URL to the proper http for unsecure SACM, proper hostname if not localhost, and correct port.

ConnectionManager

Ensure **True** is selected 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 service and support.

Dialer Specify details about your modem and service and support connection parameters.

Machines

Add two SA client servers.

Enroll Register the servers with service and support. This initiates a call to service and support to enroll the servers in service and support's database. To complete the process, service and support sends the SA gateway database a key for each enrolled host. Your common IBM ID also will be associated with the newly enrolled host.

Call log

Check the status of the call to service and support. You can see whether the call to service and support is successful.

If you are using AIX V5R3 or earlier or are using Linux, 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.

If you are using AIX V5R3.J or later or are using Linux, to learn about advanced features that go beyond the scope of this example, go to Electronic Service Agent in the IBM Systems Software Information Center.

Related information

-  [Electronic Service Agent Web site](#)

Task 11. Register the ID with Electronic Service Agent for AIX or Linux:

1. From the Service Agent Basic User Interface, click **Enroll**.
2. Complete the required fields on the right side of the interface. Required fields are indicated with an exclamation point.
3. Continue with "Task 12. Configure the service processor."

Task 12. Configure the service processor:

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.

Note: If you are using a 7037-A50 or 7047-185 server, this task does not apply. Continue with “Task 11. Register the ID with Electronic Service Agent for AIX or Linux” on page 64.

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

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.

Note: To perform these tasks, you must have an authority level of either Administrator or Service provider.

2. In the navigation area, expand **System Service Aids**.
3. To configure the service processor system port, follow these steps:
 - a. Select **Serial Port Setup**.
 - b. Modify the appropriate fields in the S1 (used with the call-home feature) and S2 (used with the call-in feature) sections.
 - c. Click **Save settings** to save the setting changes.
4. To configure the modem, follow these steps:
 - a. Select **Modem Configuration**.
 - b. Modify the appropriate fields in the S1 and S2 sections.
 - c. Click **Save settings**.
5. To configure the call-home and call-in policy, follow these steps:
 - a. Select **Call-in/Call-home**.
 - b. Enter the desired text into the specified fields.
 - c. Click **Save settings** to save changes.
6. To test the call-home policy, follow these steps:
 - a. Select **Call-Home Test**.
 - b. Click **Initiate call-home test**. A test of the call-home system is performed as specified by the current port and modem selections.
7. Continue with “Task 13. Test the connection to service and support.”

Related concepts

“Enabling remote support without an HMC when you have AIX or Linux” on page 103

Use this information to learn how to enable remote support when you do not have an HMC and you have AIX or Linux.

Task 13. Test the connection to service and support:

1. To test the connection for AIX (if you set up Electronic Service Agent on the server or logical partition), follow these steps:
 - a. Ensure that the Electronic Service Agent Connection Manager is active if it is located on a machine other than the Electronic Service Agent server.
 - b. From SMIT, start the Service Agent Advanced User Interface.
 - c. Open the **Manual Tools** folder.
 - d. Select **Connect**.
 - e. Monitor the CallLog for the following entry: TEST Connection (Success: 1, Fail: 0).
2. To test the connection for Linux (if you set up Electronic Service Agent on the server or logical partition), follow these steps:

- a. Ensure that the Electronic Service Agent Connection Manager is active if it is located on a machine other than the Electronic Service Agent server.
- b. Start the Service Agent Advanced User Interface.
- c. At a Linux command prompt, type one of the following depending on whether you want the user interface or ASCII:
`/usr/svcagent/bin/sau`

`or`
`/usr/svcagent/bin/sauascii`
- d. Open the **Manual Tools** folder.
- e. Click **Connection**.
- f. Monitor the CallLog for the following entry: TEST Connection (Success: 1, Fail: 0).

Task 14. View the server information that was reported:

You can use the Internet to view details of the system you have enabled, and see the data collected by Electronic Service Agent. To use the advanced features and receive the full benefits of Electronic Service Agent, you must enter an IBM Registration ID (IBM ID). The first IBM ID entered will have Administrator authority and is able to authorize additional users on the Web site. The second IBM ID is available as a backup for the Administrator.

1. Go to the IBM Electronic Service Agent Web site.
 2. Click **Sign in** (in the upper-right corner).
 3. Type the IBM ID and password.
 4. Choose the following options from the navigation bar:
 - To view your server information, click **My systems**.
 - To search technical support using your server information to improve the search results, click **Premium Search**.
- Note:** In some cases, the Premium Search feature is available only while your server is under warranty or afterward through a service contract.
- To view information related to your servers and interests, click **My messages**.
5. Enter the requested information.

Related information

 [Electronic Service Agent Web site](#)

Setting up IBM i5/OS to connect to service and support with an HMC

Learn about all the tasks you need to perform to set up connectivity to service and support from i5/OS logical partitions and servers.

Perform or verify Tasks 1 through 14 to set up connectivity for an i5/OS logical partition or server with an HMC.

Task 1. Before you begin:

This procedure contains the complete list of tasks needed to set up connectivity to service and support. Some of these tasks might already have been completed (during initial server setup, for example). If so, you can use this procedure to verify that the tasks were completed correctly.

In this document, an *Internet connection* is defined as access to the Internet from a logical partition, server, or HMC by direct or indirect access. *Indirect* means that you are behind a Network Address Translation (NAT) firewall. *Direct* means that you have a globally routable address without an intervening firewall, which would block the ports that are needed for communication to service and support.

Task 2. Decide on your connectivity method:

Choose the method that best describes your situation.

If you have an HMC and have multiple logical partitions:

- For the HMC, use one of the following methods:
 - Direct Internet including VPN or a Secure Sockets Layer (SSL) connection
 - Shared direct Internet
 - Shared dial-up connection

Note: If you have multiple HMCs on the same subnet, or HMCs that manage common systems, only one HMC needs to connect to service and support. This allows connectivity to be concentrated through one HMC which simplifies firewall rules.

- For i5/OS logical partitions or servers, use one of the following methods (listed in the recommended order):
 - Direct Internet (including VPN or an HTTP(S) from each logical partition or server
 - Shared direct Internet through one of the i5/OS partitions or servers
 - Shared dial-up connection through one of the i5/OS logical partitions or servers
 - Shared dial-up through the HMC's modem

Note: For i5/OS, in addition to the connectivity methods above, you can configure connectivity through an HTTP proxy. You also can configure a primary and backup method. For example, you could have direct Internet as your *primary* method, and shared dialup as your *backup* method.

Task 3. Prerequisites:

1. For direct Internet connections, contact the network administrator to verify the following:
 - For HMC environments, and for i5 servers in a non-HMC environment, if you plan on using VPN for transport, ensure that the following ports are open for communication:
 - Protocol UDP ports 500 and 4500 with the following IP addresses: 207.25.252.196 and 129.42.160.16
 - ESP (protocol 50) with the following IP addresses: 207.25.252.196 and 129.42.160.16
 - For HMC environments, if you plan on using Secure Sockets Layer for transport and a firewall is in place between the HMC and the Internet, it must allow outgoing TCP/IP connections on port 443 from the HMC to each of the following IP addresses:
 - 129.42.160.48 and 207.25.252.200 (all regions)
 - 129.42.160.49 and 207.25.252.204 (North or South America)
 - 129.42.160.50 and 207.25.252.205 (all other regions)

Note: You need to specify only the IP addresses necessary to set up access that is appropriate for your region.

- For i5/OS, if you plan to use HTTP and HTTPs for transport, you must change the filter rules to allow connections to the IBM service destinations for ports 80 and 443. For more details, see IP Packet Filter Firewall.
 - If multiple logical partitions are sharing an Internet connection, you will need the IP addresses or host names created for TCP/IP and for virtual Ethernet.
2. For a dial-up (modem) connection, determine necessary configuration settings, including:
 - Local area code
 - Predial information, such as dialing 9 to dial outside the network
 - Use of commas if delayed dialing is needed
 - Any special telephone line conditions such as pulse (rotary) dialing or no dialtone.

3. Ensure that TCP/IP is set up and configured correctly. If not, contact the network administrator and consult your operating system documentation.

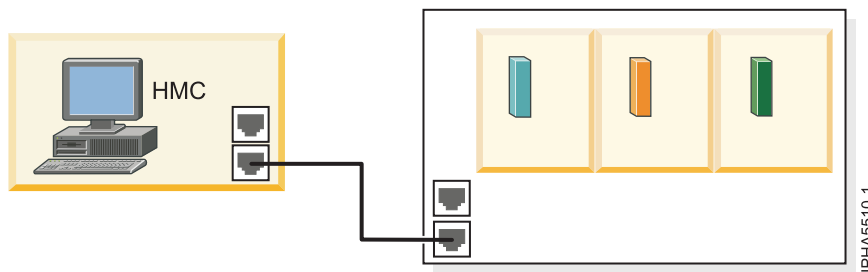
Task 4. Ensure that your physical networking is set up correctly:

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 updates:

- Between the service processor and the HMC
 - Between your site and service and support
1. Verify the physical connection between the service processor and the HMC.

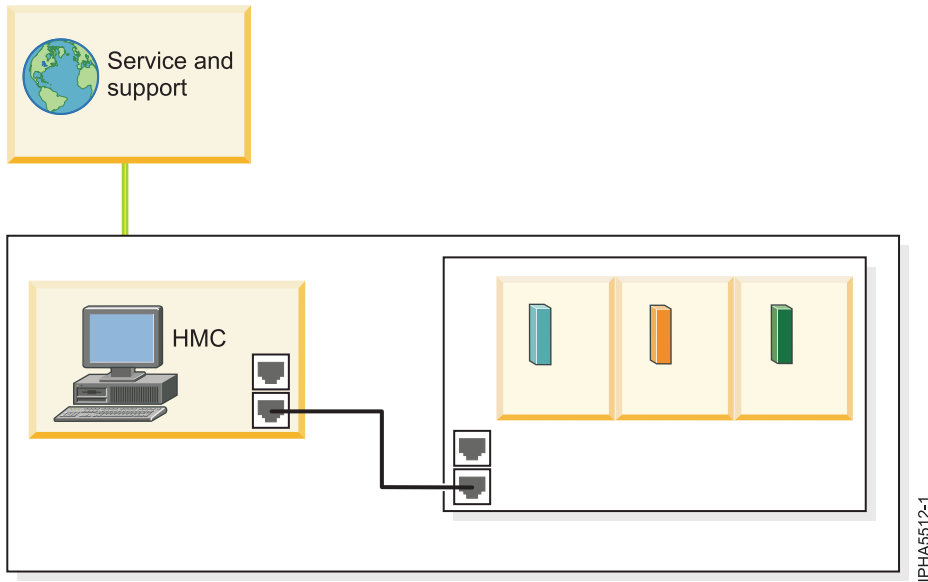
The service processor is part of your platform hardware and monitors hardware attributes and conditions on your server. The service processor is controlled by server firmware and does not require an operating system to perform its tasks. The connection to the service processor is recommended for all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

Figure 31. This diagram shows the Ethernet connection between your HMC and the service processor on your server.



2. Verify the physical connection from your site to service and support.
- This connection enables you to report hardware problems and other server information to service and support. It also enables you to install updates. This connection is represented in the following illustration:

Figure 32. This diagram shows the connection between service and support and a company that has a server and an HMC.



Task 5. Obtain or verify an IBM ID:

You will need an IBM ID to register IBM Electronic Service Agent on the HMC and for Electronic Service Agent on your operating system or systems. You also will need this ID to view information that has been reported to IBM through Electronic Service Agent.

1. Go to the My IBM Profile Web site.
2. Verify that you are registered.
 - If you are registered, Welcome back will be displayed on the Web site. Or, you can select **Sign in** and see if your e-mail address is recognized.
 - If you are not registered, select **Register** and fill out the registration form. Create an IBM ID for each of the people you want to have access to the information that Electronic Service Agent reports to IBM. You must associate these accounts with a server, usually your central server. (You can add other servers later.) The people for whom you create IDs must have system administrator authority on all registered servers.
3. Record your IBM ID (the e-mail address that you registered).
4. You will need the ID during "Task 6. Verify the HMC service settings."

Task 6. Verify the HMC service settings:

To verify that the HMC service settings are set up correctly, use the Guided Setup wizard.

Note: If you have not set up your server, do that now. For details, refer to Initial server setup.

1. Access the Guided Setup wizard using the HMC interface:
 - a. In the navigation area, select the HMC that you want to work with.
 - b. Click **Information Center and Setup Wizard**.
 - c. In the contents pane, click **Launch the Guided Setup Wizard**. 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.
2. Click **Next** to skip the tasks that are not specific to setting up service, including:
 - 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
3. Ensure that the following service tasks are completed correctly:
 - a. Customer contact information for service-related activities, including:
 - Company name
 - Administrator name
 - E-mail address
 - Telephone numbers
 - Information regarding the location of the HMC
 - b. Configuration of connectivity for service-related activities.
 - **Internet VPN**

Note: When configuring the HMC's network settings for connecting using direct or indirect Internet, the HMC must be configured with a default gateway to access the Internet. Select **HMC Management > HMC Configuration > Customize Network Settings**. Ensure that the Default Gateway Information field has a Gateway address listed and a selection is made in the Gateway device field (for example, any).

- **Internet:** Currently, the SSL option must be configured manually:
 - 1) Select **Service Applications → Remote Support → Customize Outbound Connectivity**
 - 2) Select the **Internet** tab.
 - **Dial-up connection from the local HMC**
 - **Connecting through other systems or logical partitions**
- c. Configuration of the network settings.
 - For direct or indirect Internet:
 - HMC host name
 - Domain name
 - Description of HMC
 - For a dial-up modem connection:
 - Dial prefix, if applicable
 - Modem configuration, including:
 - Dial type
 - Dial prefix, if applicable
 - Telephone number
 - d. Authorize two users for Electronic Service Agent by entering the ID (the e-mail address that you registered with the My Profile Web site at <https://www.ibm.com/account/profile>).

Note: You will be able to authorize more users later.

- e. Add e-mail addresses for those you want to be notified when problem events occur.
4. To test the connection from the HMC, open **Service Applications → Remote Support → Customize Outbound Connectivity**.
5. Select the tab for the type of outbound connectivity that you chose for your HMC (Local Modem, Internet, Internet VPN, or Pass-Through Systems). For more information about these settings, see Choosing your connection method.
6. Click **Test**.
7. Choose from the following options:
 - If the test is successful, continue with the next Task.
 - If the test fails, continue with the next step.

8. Ensure that your country or region is listed. Select **Service Applications** → **Remote Support** → **Customize Customer Information**. Ensure that your country or region is selected from the list.
9. Choose from the following options:
 - If you have a dial-up connection, perform the following:
 - Check the telephone line going into the HMC and the wall socket.
 - Check to make sure that you have the telephone number configured correctly, including predial information, such as dialing 9 to dial outside the network.
 - If you have an Internet VPN connection, perform the following:
 - Ensure that the appropriate firewall rules have been added, if necessary.
 - Check that you have a default gateway set up on the HMC. Select **HMC Management** → **HMC Configuration** → **Customize Network Settings**. Ensure that the Default Gateway Information field has a Gateway address listed and a selection is made in the Gateway device field (for example, any).

Task 7. Set up and configure your logical partitions:

For details, refer to Partitioning the server.

Task 8. Install the operating systems on your server or logical partitions:

For details, refer to Installing operating systems.

Task 9. Configure your TCP/IP network:

For instructions, refer to the operating system documentation.

Task 10. Activate TCP/IP on your server or logical partitions:

TCP/IP starts automatically, as long as the network adapter is recognized and can communicate with the network when the i5/OS operating system is started. If this does not occur, type STRTCP at an i5/OS command line to start TCP/IP. This command initializes and activates TCP/IP processing, starts the TCP/IP interfaces, and starts the server jobs. Only TCP/IP interfaces and servers with AUTOSTART *YES are started with the STRTCP command.

Task 11. Configure Electronic Service Agent for i5/OS:

1. Ensure that the following software is installed (use the DSPSFWRSC command to confirm).

Note: Electronic Service Agent and the following software is included with the base i5/OS operating system starting with V5R3.

- 5722SS1 – Option 34 (OS/400® - Digital Certificate Manager)
- If you have i5/OS V5R3, you will need 5722AC3 (Cryptographic Access Provider 128-bit). This is a security provision to encrypt communications between your system and service and support.

Note: The 5722AC3 (Cryptographic Access Provider 128-bit) is not necessary starting with i5/OS V5R4.

- 5722JC1 (IBM Toolbox Kit for Java™)
2. At the command line, type G0 SERVICE. One of the following occurs:
 - If connectivity was set up previously, type 18 to get to the configuration menu where you can create, change, delete, or verify that connectivity works. If you want to change the settings, continue with step 3 on page 72.
 - If connectivity has never been set up on this logical partition or server, it will try to ping one of the IBM gateways. If this is successful, the interface will prompt for configuring direct Internet. If

this is successful, the default settings for direct Internet will be pre-filled. If you want to verify or change these default settings, continue with step 3.

Note: In some environments, the pinging of the IBM gateway does not work because the firewall might be blocking the packets. However, you should still verify with the network administrator if the criteria is met to set up direct Internet. For details, see “Task 1. Before you begin” on page 66.

3. Choose from the following options:
 - To set up a direct Internet connection from each i5/OS server or logical partition, go to step 4.
 - To set up a shared direct Internet connection, go to step 6.
 - To set up a modem or shared modem connection, go to step 11 on page 74.
 - To set up a connection through the modem on the HMC, go to step 17 on page 75.

4. To set up a direct Internet connection from each i5/OS server or logical partition, specify the following information from each logical partition in the CRTSRVCFG prompts:

For i5/OS V5R3:

- Connection type: *VPN
- Virtual private network type: *DIRECT
- Connectivity for others: Connect point: *NO

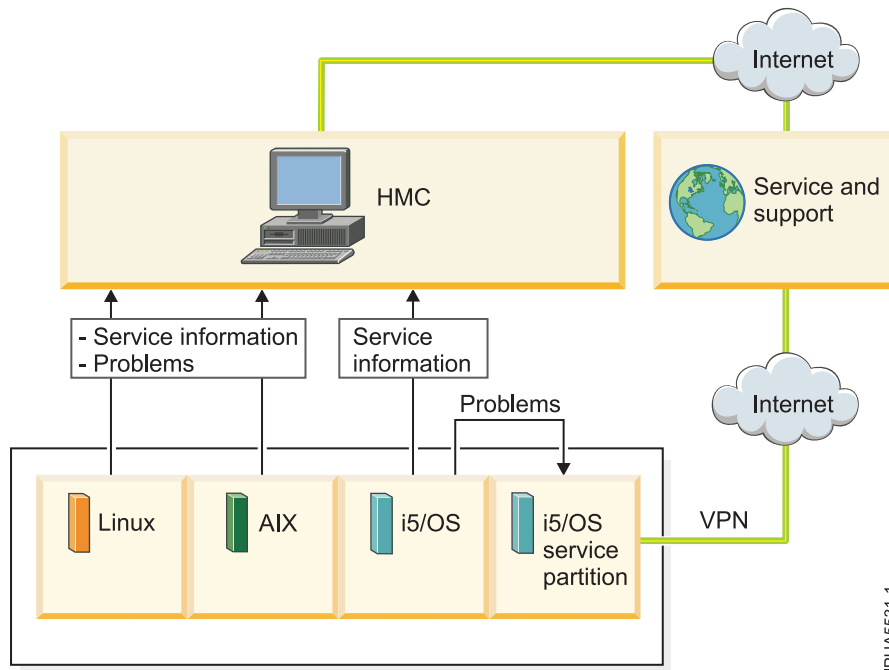
For i5/OS V5R4:

- Role: *PRIMARY
- Connection type: *DIRECT
- Connectivity for others: Connect point: *NO

Note: For additional details on using Electronic Service Agent, refer to the Electronic Service Agent topic in the iSeries Information Center.

5. Continue with “Task 12. Register the IBM ID for i5/OS” on page 76.
6. To set up a shared direct Internet connection, review the following information.
 - A direct Internet connection from the i5/OS logical partition that has connectivity to the Internet.
 - Enable the other logical partitions to connect to the logical partition that has connectivity to the Internet

Figure 33. This diagram shows the flow of information and problems from four logical partitions and the HMC to service and support. The service information passes through the HMC to service and support over a direct Internet connection. And, problems from i5/OS pass through the i5/OS logical partition to service and support.



7. Specify the following information from the i5/OS server or logical partition with Internet connectivity in the CRTSRVCFG prompts:

For i5/OS V5R3:

- Connection type: *VPN
- Virtual private network type: *DIRECT
- Connectivity for others:
 - Connect point: *YES. This enables other logical partitions or systems to use the VPN connection on this logical partition to connect to service and support.

Note: You will need to create service configurations on the remote systems or logical partitions that will be using this connection point.

- Interfaces: *ALL or a list of the interfaces over which you will accept connections to service and support.

For i5/OS V5R4:

- Role: *PRIMARY
- Connection type: *DIRECT
- Connectivity for others:
 - Connect point: *YES. This enables other logical partitions or systems to use the VPN or service and support proxy connection on this logical partition to connect to service and support.

Note: Service configurations need to be created on the remote systems or logical partitions that will be using this connection point.

- Interfaces: *ALL or a list of the interfaces over which you will accept connections to service and support.

8. Specify the following information from each of the other i5/OS server or logical partitions in the CRTSRVCFG prompts:

For V5R3 i5/OS:

- Connection type: *VPN
- Virtual private network type: *MULTIHOP

- Remote system: Enter the host name or IP address of the logical partition with the Internet connectivity.

Note: A multi-hop VPN connection from an i5/OS system or logical partition using the IP address of the HMC is not supported. The only connectivity option for an i5/OS logical partition to the HMC is to use a remote PTP configuration.

- Connectivity for others: Connect point: *NO

For i5/OS V5R4:

- Connection type: *MULTIHOP
- Remote system: Enter the host name or IP address of the logical partition with the Internet connectivity.

Note: A multi-hop VPN connection from an i5/OS system or logical partition using the IP address of the HMC is not supported. The only connectivity option for an i5/OS logical partition to the HMC is to use a remote PTP configuration.

- Proxy server: Enter the information about the Service and Support Proxy (or your own HTTP proxy) as follows:
 - IP address or host name: Enter the host name or IP address of the logical partition with the Internet connectivity (or if you have your own HTTP proxy, you could also specify that).
 - Port number: Enter the port number of the Service and Support proxy or your own HTTP proxy. Default of *IBMSVR which is 5026 (the default for the Service and Support proxy).
 - Relative priority: Enter the priority (relative to the multi-hop VPN)
- Connectivity for others: Connect point: *NO

9. Verify that interpartition communication is set up. Ping the host or IP address of the logical partition that has the Internet connectivity or modem from the logical partition that needs to use the Internet connection or modem.

Note: For additional details on using Electronic Service Agent, refer to the Electronic Service Agent topic in the iSeries Information Center.

10. Continue with “Task 12. Register the IBM ID for i5/OS” on page 76.
11. To set up a modem or shared modem on your i5/OS server or logical partition, choose from the following options:
 - To set up a modem from an i5/OS server or logical partition, go to step 12.
 - To set up a shared modem for an i5/OS server or logical partition, go to step 14.
12. To set up a modem from an i5/OS server or logical partition, specify the following options from the server in the CRTSRVCFG prompts:

For i5/OS V5R3:

- Connection type: *PTP
- Virtual private network type: *LOCAL
- Service: *SRVAGT

For i5/OS V5R4:

- Connection type: *LCLDIAL
- Connectivity for others: Connect point: *NO

Note: For additional details on using Electronic Service Agent, refer to the Electronic Service Agent topic in the iSeries Information Center.

13. Continue with “Task 12. Register the IBM ID for i5/OS” on page 76.
14. To set up a shared modem (you have multiple systems or logical partitions), specify the following information from the system or logical partition with the modem in the CRTSRVCFG prompts:

For i5/OS V5R3:

- Connection type: *PTP
- Virtual private network type: *LOCAL
- Service: *SRVAGT
- Connectivity for others:
 - Connect point: *YES: This enables other logical partitions or systems to use the PTP dial connection on this logical partition to connect to service and support.

Note: Service configurations need to be created on the remote systems or logical partitions that will be using this connection point.

- Interfaces: *ALL or a list of the interfaces over which you will accept connections to service and support.

For i5/OS V5R4:

- Connection type: *LCLDIAL
- Connectivity for others:
 - Connect point: *YES: This enables other logical partitions or systems to use the dial connection on this logical partition to connect to service and support.

Note: Service configurations need to be created on the remote systems or logical partitions that will be using this connection point.

- Interfaces: *ALL or a list of the interfaces over which you will accept connections to service and support.

15. Specify the following information from each of the other i5/OS servers or logical partitions in the CRTSRVCFG prompts:

For i5/OS V5R3:

- Connection type: *PTP
- Point to point type: *REMOTE
- Service: *SRVAGT
- Remote system: Enter the host name or IP address of the system or logical partition with the modem.

For i5/OS V5R4:

- Connection type: *RMTDIAL
- Remote system: Enter the host name or IP address of the system or logical partition with the modem.

Note: For additional details on using Electronic Service Agent, refer to the Electronic Service Agent topic in the iSeries Information Center.

16. Continue with “Task 12. Register the IBM ID for i5/OS” on page 76.

17. To set up a connection from an i5/OS server or logical partition through the HMC’s modem, specify the following information in the CRTSRVCFG prompts from each logical partition that will use the HMC’s modem:

For i5/OS V5R3:

- Connection type: *PTP
- Point to point type: *REMOTE
- Service: *SRVAGT
- Remote system: Enter the IP address or host name of the interface on the HMC through which you will connect to service and support.

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, continue with the next step.

For i5/OS V5R4:

- Connection type: *RMTDIAL
- Remote system: Enter the IP address or host name of the interface on the HMC through which you will connect to service and support.

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, continue with the next step.

18. To find the interface that provides partition communication, follow these steps from the HMC interface:
 - a. In the navigation area, expand the HMC you want to work with. The HMCs are listed by host name or IP address.
 - b. Expand **HMC Management**.
 - c. Click **HMC Configuration**.
 - d. In the contents pane, click **Customize network settings**.
 - e. Click the **LAN Adapters** tab.
 - f. Select a LAN adapter and click **Details**.
 - g. Click the **Lan Adapter** tab. In the Local Area Network Information section, the Partition communication checkbox indicates whether this interface is used for partition communication.

Note: For additional details on using Electronic Service Agent, refer to the Electronic Service Agent topic in the iSeries Information Center.

19. Continue with "Task 12. Register the IBM ID for i5/OS."

Task 12. Register the IBM ID for i5/OS:

Register the IBM ID with Electronic Service Agent for i5/OS by following these steps:

1. At the i5/OS command line, type **GO SERVICE**.
2. From the Electronic Service Agent menu, select **Authorize users to access service information** and press Enter.
3. Type your IBM ID (internet address that you registered with the My Profile Web site at <https://www.ibm.com/account/profile>) in the Authorize users field and press Enter.
4. Continue with "Task 13. Test the connection to service and support"

Task 13. Test the connection to service and support:

1. If you use an HMC to connect to service and support, follow these steps to test the connection for the HMC:
 - a. On the HMC, open **Service Applications > Service Focal Point > Service Utilities**.
 - b. Select a system.
 - c. Select **Selected > Create serviceable event**.
 - d. Select **Test automatic problem reporting**.
 - e. Select **Request Service**. A message is displayed when the service request is sent.
2. To test the connection for i5/OS servers or logical partitions, perform the following steps.
 - a. To test the Electronic Service Agent connection, enter the following command at the command line:

GO SERVICE

- b. From the Electronic Service Agent menu, select option 17 (Verify Service Configuration), and press Enter. A message is displayed that indicates whether the test connection is successful.
- c. To test the electronic customer support connection profile, enter the following command:
SNDSRVRQS *TEST

A message is displayed that indicates whether the test connection is successful.

Task 14. View the server information that was reported to IBM:

You can use the Internet to view details of the system you have enabled, and see the data collected by Electronic Service Agent. To use the advanced features and receive the full benefits of Electronic Service Agent, you must enter an IBM Registration ID (IBM ID). The first IBM ID entered will have Administrator authority and is able to authorize additional users on the Web site. The second IBM ID is available as a backup for the Administrator.

1. Go to the IBM Electronic Services Web site.
2. Click **Sign in** (in the upper-right corner).
3. Type the IBM ID and password.
4. Choose the following options from the navigation bar:
 - To view your server information, click **My systems**.
 - To search technical support using your server information to improve the search results, click **Premium Search**.

Note: In some cases, the Premium Search feature is available only while your server is under warranty or afterward through a service contract.

- To view information related to your servers and interests, click **My messages**.
5. Enter the requested information.

Setting up IBM i5/OS to connect to service and support without an HMC

Learn about all the tasks you need to perform for setting up connectivity to service and support from i5/OS servers.

Perform or verify Tasks 1 through 12 to set up connectivity for an i5/OS server.

Task 1. Before you begin:

This procedure contains the complete list of tasks needed to set up connectivity to service and support. Some of these tasks might already have been completed (during initial server setup, for example). If so, you can use this procedure to verify that the tasks were completed correctly.

In this document, an *Internet connection* is defined as access to the Internet from a logical partition, server, or HMC by direct or indirect access. *Indirect* means that you are behind a Network Address Translation (NAT) firewall. *Direct* means that you have a globally routable address without an intervening firewall, which would block the ports that are needed for communication to service and support.

Task 2. Decide on your connectivity method:

Use one of the following methods (listed in the recommended order):

Note: See below for details on each option.

- Direct Internet (including VPN or an HTTP(S) from each logical partition or server
- Shared direct Internet through one of the i5/OS partitions or servers
- Shared dial-up connection through one of the i5/OS logical partitions or servers

- Shared dial-up through the HMC's modem

Note: For i5/OS, in addition to the connectivity methods above, you can configure connectivity through an HTTP proxy. You also can configure a primary and backup method. For example, you could have direct Internet as your *primary* method, and shared dialup as your *backup* method.

Task 3. Prerequisites:

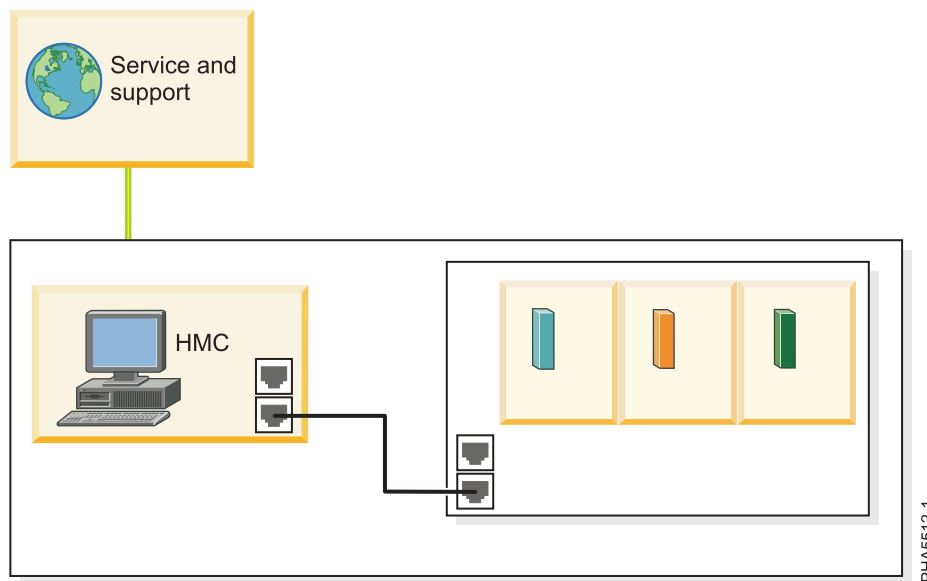
1. For direct Internet connections, contact the network administrator to verify that the following ports are open for communication:
 - Protocol UDP ports 500 and 4500 with the following IP addresses: Boulder: 207.25.252.196 and Rochester: 129.42.160.16
 - ESP (protocol 50) with the following IP addresses: Boulder: 207.25.252.196 and Rochester: 129.42.160.16
 - If you plan to use HTTP and HTTPS for a transport, you must change the filter rules to allow connections to the IBM service destinations for ports 80 and 443. For more details, see “IP Packet Filter Firewall” on page 114.
2. For a dial-up (modem) connection, determine necessary configuration settings, including:
 - Local area code
 - Predial information, such as dialing 9 to dial outside the network
 - Use of commas if delayed dialing is needed
 - Any special telephone line conditions such as pulse (rotary) dialing or no dialtone.
3. Ensure that TCP/IP is set up and configured correctly. If not, contact the network administrator and consult your operating system documentation.

Task 4. Ensure that your physical networking is set up correctly:

1. Verify the physical connection from your site to service and support.

This connection enables you to report hardware problems and other server information to service and support. It also enables you to install updates. This connection is represented in the following illustration:

Figure 34. This diagram shows the connection between service and support and a company that has a server and an HMC.



2. Continue with "Task 5. Obtain or verify an IBM ID."

Task 5. Obtain or verify an IBM ID:

You will need an IBM ID to register IBM Electronic Service Agent on the HMC and for Electronic Service Agent on your operating system or systems. You also will need this ID to view information that has been reported to IBM through Electronic Service Agent.

1. Go to the My IBM Profile Web site.
2. Verify that you are registered.
 - If you are registered, Welcome back will be displayed on the Web site. Or, you can select **Sign in** and see if your e-mail address is recognized.
 - If you are not registered, select **Register** and fill out the registration form. Create an IBM ID for each of the people you want to have access to the information that Electronic Service Agent reports to IBM. You must associate these accounts with a server, usually your central server. (You can add other servers later.) The people for whom you create IDs must have system administrator authority on all registered servers.
3. Record your IBM ID (the e-mail address that you registered).

Task 6. Install the operating systems on your server:

For details, refer to Installing operating systems.

Task 7. Configure your TCP/IP network:

For instructions, refer to the operating system documentation.

Task 8. Activate TCP/IP on your server or logical partitions:

TCP/IP starts automatically, as long as the network adapter is recognized and can communicate with the network when the i5/OS operating system is started. If this does not occur, type STRTCP at an i5/OS command line to start TCP/IP. This command initializes and activates TCP/IP processing, starts the TCP/IP interfaces, and starts the server jobs. Only TCP/IP interfaces and servers with AUTOSTART *YES are started with the STRTCP command.

Task 9. Configure Electronic Service Agent for i5/OS:

1. Ensure that the following software is installed (use the DSPSFWRSC command to confirm).

Note: Electronic Service Agent and the following software is included with the base i5/OS operating system starting with V5R3.

- 5722SS1 – Option 34 (OS/400 - Digital Certificate Manager)
- If you have i5/OS V5R3, you will need 5722AC3 (Cryptographic Access Provider 128-bit). This is a security provision to encrypt communications between your system and service and support.

Note: The 5722AC3 (Cryptographic Access Provider 128-bit) is not necessary starting with i5/OS V5R4.

- 5722JC1 (IBM Toolbox Kit for Java)
2. At the command line, type G0 SERVICE. One of the following occurs:
 - If connectivity was set up previously, type 18 to get to the configuration menu where you can create, change, delete, or verify that connectivity works. If you want to change the settings, continue with step 3 on page 80.
 - If connectivity has never been set up on this logical partition or server, the system will try to ping one of the IBM gateways. If this is successful, the interface will prompt for configuring direct

Internet. If this is successful, the default settings for direct Internet will be prefilled. If you want to verify or change these default settings, continue with step 3.

Note: In some environments, the pinging of the IBM gateway does not work because the firewall might be blocking the packets. However, you should still verify with the network administrator if the criteria is met to set up direct Internet. For details, see “Task 1. Before you begin” on page 77.

3. Choose from the following options:
 - To set up a direct Internet connection from each i5/OS server, go to step 4.
 - To set up a shared direct Internet connection, go to step 6.
 - To set up a modem or shared modem connection, go to step 11 on page 82.
4. To set up a direct Internet connection from each i5/OS server or logical partition, specify the following information from each logical partition in the CRTSRVCFG prompts:

For i5/OS V5R3:

- Connection type: *VPN
- Virtual private network type: *DIRECT
- Connectivity for others: Connect point: *NO

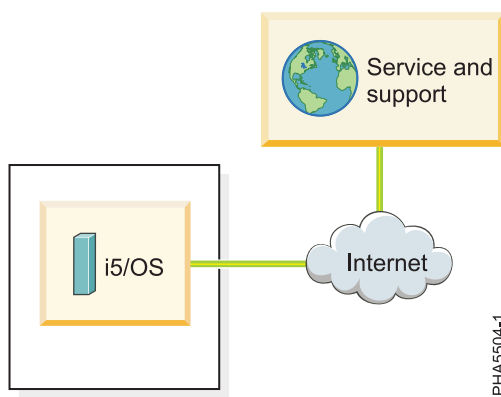
For i5/OS V5R4:

- Role: *PRIMARY
- Connection type: *DIRECT
- Connectivity for others: Connect point: *NO

Note: For additional details on using Electronic Service Agent, refer to the Electronic Service Agent topic in the iSeries Information Center.

5. Continue with “Task 10. Register the IBM ID for i5/OS” on page 83.
6. To set up a shared direct Internet connection, review the following information. In this example, you will configure the following:
 - A direct Internet connection from the i5/OS server that has connectivity to the Internet.
 - Enable the other i5/OS server to connect to the server that has connectivity to the Internet.

Figure 35. This diagram shows the flow of information and problems from an i5/OS server in its manufacturing default configuration to service and support. The information and problems pass through the direct Internet connection on the server.



7. Specify the following information from the i5/OS server or logical partition with Internet connectivity in the CRTSRVCFG prompts:

For i5/OS V5R3:

- Connection type: *VPN

- Virtual private network type: *DIRECT
- Connectivity for others:
 - Connect point: *YES. This enables other logical partitions or systems to use the VPN connection on this logical partition to connect to service and support.

Note: You will need to create service configurations on the remote systems or logical partitions that will be using this connection point.

- Interfaces: *ALL or a list of the interfaces over which you will accept connections to service and support.

For i5/OS V5R4:

- Role: *PRIMARY
- Connection type: *DIRECT
- Connectivity for others:
 - Connect point: *YES. This enables other logical partitions or systems to use the VPN or service and support proxy connection on this logical partition to connect to service and support.

Note: Service configurations need to be created on the remote systems or logical partitions that will be using this connection point.

- Interfaces: *ALL or a list of the interfaces over which you will accept connections to service and support.

8. Specify the following information from each of the other i5/OS server or logical partitions in the CRTSRVCFG prompts:

For V5R3 i5/OS:

- Connection type: *VPN
- Virtual private network type: *MULTIHOP
- Remote system: Enter the host name or IP address of the logical partition with the Internet connectivity.

Note: A multi-hop VPN connection from an i5/OS system or logical partition using the IP address of the HMC is not supported. The only connectivity option for an i5/OS logical partition to the HMC is to use a remote PTP configuration.

- Connectivity for others: Connect point: *NO

For i5/OS V5R4:

- Connection type: *MULTIHOP
- Remote system: Enter the host name or IP address of the logical partition with the Internet connectivity.

Note: A multi-hop VPN connection from an i5/OS system or logical partition using the IP address of the HMC is not supported. The only connectivity option for an i5/OS logical partition to the HMC is to use a remote PTP configuration.

- Proxy server: Enter the information about the Service and Support Proxy (or your own HTTP proxy) as follows:
 - IP address or host name: Enter the host name or IP address of the logical partition with the Internet connectivity (or if you have your own HTTP proxy, you could also specify that).
 - Port number: Enter the port number of the Service and Support proxy or your own HTTP proxy. Default of *IBMSVR which is 5026 (the default for the Service and Support proxy).
 - Relative priority: Enter the priority (relative to the multi-hop VPN)
- Connectivity for others: Connect point: *NO

9. Verify that interpartition communication is set up. Ping the host or IP address of the logical partition that has the Internet connectivity or modem from the logical partition that needs to use the Internet connection or modem.

Note: For additional details on using Electronic Service Agent, refer to the Electronic Service Agent topic in the iSeries Information Center.

10. Continue with “Task 10. Register the IBM ID for i5/OS” on page 83.
11. To set up a modem or shared modem on your i5/OS server or logical partition, choose from the following options:
 - To set up a modem from an i5/OS server, continue with the next step.
 - To set up a shared modem, go to step 14.
12. To set up a modem from an i5/OS server or logical partition, specify the following options from the server in the CRTSRVCFG prompts:

For i5/OS V5R3:

 - Connection type: *PTP
 - Virtual private network type: *LOCAL
 - Service: *SRVAGT

For i5/OS V5R4:

 - Connection type: *LCLDIAL
 - Connectivity for others: Connect point: *NO

Note: For additional details on using Electronic Service Agent, refer to the Electronic Service Agent topic in the iSeries Information Center.

13. Continue with “Task 12. View the server information that was reported to IBM” on page 83.
14. To set up a shared modem (you have multiple systems or logical partitions), specify the following information from the system or logical partition with the modem in the CRTSRVCFG prompts:

For i5/OS V5R3:

 - Connection type: *PTP
 - Virtual private network type: *LOCAL
 - Service: *SRVAGT
 - Connectivity for others:
 - Connect point: *YES: This enables other logical partitions or systems to use the PTP dial connection on this logical partition to connect to service and support.

Note: Service configurations need to be created on the remote systems or logical partitions that will be using this connection point.

- Interfaces: *ALL or a list of the interfaces over which you will accept connections to service and support.

For i5/OS V5R4:

- Connection type: *LCLDIAL
- Connectivity for others:
 - Connect point: *YES: This enables other logical partitions or systems to use the dial connection on this logical partition to connect to service and support.

Note: Service configurations need to be created on the remote systems or logical partitions that will be using this connection point.

- Interfaces: *ALL or a list of the interfaces over which you will accept connections to service and support.

15. Specify the following information from each of the other i5/OS servers or logical partitions in the CRTSRVCFG prompts:

For i5/OS V5R3:

- Connection type: *PTP
- Point to point type: *REMOTE
- Service: *SRVAGT
- Remote system: Enter the host name or IP address of the system or logical partition with the modem.

For i5/OS V5R4:

- Connection type: *RMTDIAL
- Remote system: Enter the host name or IP address of the system or logical partition with the modem.

Note: For additional details on using Electronic Service Agent, refer to the Electronic Service Agent topic in the iSeries Information Center.

Task 10. Register the IBM ID for i5/OS:

Register the IBM ID with Electronic Service Agent for i5/OS by following these steps:

1. At the i5/OS command line, type GO SERVICE.
2. From the Electronic Service Agent menu, select **Authorize users to access service information** and press Enter.
3. Type your IBM ID (internet address that you registered with the My Profile Web site at <https://www.ibm.com/account/profile>) in the Authorize users field and press Enter.

Task 11. Test the connection to service and support:

To test the connection for i5/OS servers or logical partitions, perform the following steps.

1. To test the Electronic Service Agent connection, enter the following command at the command line:
GO SERVICE
2. From the Electronic Service Agent menu, select option 17 (Verify Service Configuration), and press Enter. A message is displayed that indicates whether the test connection is successful.
3. To test the electronic customer support connection profile, enter the following command:
SNDSRVQRQS *TEST

A message is displayed that indicates whether the test connection is successful.

Task 12. View the server information that was reported to IBM:

You can use the Internet to view details of the system you have enabled, and see the data collected by Electronic Service Agent. To use the advanced features and receive the full benefits of Electronic Service Agent, you must enter an IBM Registration ID (IBM ID). The first IBM ID entered will have Administrator authority and is able to authorize additional users on the Web site. The second IBM ID is available as a backup for the Administrator.

1. Go to the IBM Electronic Services Web site.
2. Click **Sign in** (in the upper-right corner).
3. Type the IBM ID and password.
4. Choose the following options from the navigation bar:
 - To view your server information, click **My systems**.
 - To search technical support using your server information to improve the search results, click **Premium Search**.

Note: In some cases, the Premium Search feature is available only while your server is under warranty or afterward through a service contract.

- To view information related to your servers and interests, click **My messages**.

5. Enter the requested information.

Setting up AIX, IBM i5/OS, Linux, and the HMC to connect to service and support

Learn about all the tasks you need to perform for setting up connectivity.

If you have two or more operating systems on your server, you might prefer to use this procedure which includes instructions for AIX, i5/OS, and Linux, with or without an HMC. However, if you only have one operating system on your server, you might prefer to use one of the following procedures:

- Setting up a 7037-A50 or a 7047-185 system to connect to service and support
- Setting up a clustered environment to connect to service and support
- Setting up AIX or Linux to use an HMC to connect to service and support
- Setting up AIX or Linux to connect to service and support without an HMC
- Setting up IBM i5/OS to connect to service and support with an HMC
- Setting up IBM i5/OS to connect to service and support without an HMC

Related tasks

“Setting up a 7037-A50 or a 7047-185 system to connect to service and support” on page 31

Learn about all the tasks you need to perform to set up connectivity to service and support when you are working on a 7037-A50 or a 7047-185 system.

“Setting up a clustered environment to connect to service and support” on page 37

Learn about all the tasks you need to perform to set up connectivity to service and support when you are working in a clustered environment.

“Setting up AIX or Linux to use an HMC to connect to service and support” on page 48

Learn how to create a service connection to send service information from AIX or Linux logical partitions and servers using an HMC.

“Setting up AIX or Linux to connect to service and support without an HMC” on page 59

Learn how to create a service connection to send service information from AIX or Linux servers to service and support.

“Setting up IBM i5/OS to connect to service and support with an HMC” on page 66

Learn about all the tasks you need to perform to set up connectivity to service and support from i5/OS logical partitions and servers.

“Setting up IBM i5/OS to connect to service and support without an HMC” on page 77

Learn about all the tasks you need to perform for setting up connectivity to service and support from i5/OS servers.

Task 1. Before you begin:

This procedure contains the complete list of tasks needed to set up connectivity to service and support. Some of these tasks might already have been completed (during initial server setup, for example). If so, you can use this procedure to verify that the tasks were completed correctly.

In this document, an *Internet connection* is defined as access to the Internet from a logical partition, server, or HMC by direct or indirect access. *Indirect* means that you are behind a Network Address Translation (NAT) firewall. *Direct* means that you have a globally routable address without an intervening firewall, which would block the ports that are needed for communication to service and support.

Task 2. Decide on your connectivity method:

Choose the method that best describes your situation.

If you have an HMC and have multiple logical partitions:

- For the HMC, use one of the following methods:
 - Direct Internet including VPN or a Secure Sockets Layer (SSL) connection
 - Shared direct Internet
 - Shared dial-up connection

Note: If you have multiple HMCs on the same subnet, or HMCs that manage common systems, only one HMC needs to connect to service and support. This allows connectivity to be concentrated through one HMC which simplifies firewall rules.

- For logical partitions:
 - For AIX or Linux logical partitions, hardware errors will be reported through the HMC, using the connection method provided for the HMC.
 - For i5/OS logical partitions or servers, use one of the following methods (listed in the recommended order):
 - Direct Internet (including VPN or an HTTP(S) from each logical partition or server
 - Shared direct Internet through one of the i5/OS partitions or servers
 - Shared dial-up connection through one of the i5/OS logical partitions or servers
 - Shared dial-up through the HMC's modem

Note: For i5/OS, in addition to the connectivity methods above, you can configure connectivity through an HTTP proxy. You also can configure a primary and backup method. For example, you could have direct Internet as your *primary* method, and shared dialup as your *backup* method.

If you do not have an HMC and have AIX or Linux:

- If you do not have logical partitions, use one of the following methods:
 - Direct Internet over SSL
 - Direct dial-up connection over SSL
- If you have logical partitions and are using the Integrated Virtualization Manager to manage your server, you might want to configure the service processor to contact service and support when the server is not available. For details, refer to “Task 11.3. Configure the service processor (AIX and Linux)” on page 94.

Note: If you are using the Integrated Virtualization Manager to manage your server, check Service Focal Point for the Integrated Virtualization Manager to see if you need to contact service and support.

If you do not have an HMC and have i5/OS, use one of the following methods:

- Direct Internet or shared direct Internet
- Direct dial-up connection or a shared dial-up connection.

Note: For i5/OS, in addition to the connectivity methods above, you can configure connectivity through an HTTP proxy. You also can configure a primary and backup method. For example, you could have direct Internet as your *primary* method, and shared dialup as your *backup* method.

Task 3. Prerequisites:

1. For direct Internet connections, contact the network administrator to verify the following:
 - For HMC environments, and for i5 servers in a non-HMC environment, if you plan on using VPN for transport, ensure that the following ports are open for communication:
 - Protocol UDP ports 500 and 4500 with the following IP addresses: 207.25.252.196 and 129.42.160.16
 - ESP (protocol 50) with the following IP addresses: 207.25.252.196 and 129.42.160.16

- For HMC environments, if you plan on using Secure Sockets Layer for transport and a firewall is in place between the HMC and the Internet, it must allow outgoing TCP/IP connections on port 443 from the HMC to each of the following IP addresses:
 - 129.42.160.48 and 207.25.252.200 (all regions)
 - 129.42.160.49 and 207.25.252.204 (North or South America)
 - 129.42.160.50 and 207.25.252.205 (all other regions)

Note: You need to specify only the IP addresses necessary to set up access that is appropriate for your region.

- For i5/OS, if you plan to use HTTP and HTTPS for transport, you must change the filter rules to allow connections to the IBM service destinations for ports 80 and 443. For more details, see IP Packet Filter Firewall.
 - For IBM System p5 or IBM eServer p5 servers in a non-HMC environment, choose from the following options:
 - If HTTPS traffic is restricted, ensure that the following port is open for communication: Protocol TCP port 443 with the following IP addresses: 207.25.252.200 and 129.42.160.48
 - If an HTTP proxy is available within your network, then the Service Agent traffic can be routed to it by specifying the Proxy Type as HTTP and Proxy Port as 80.
 - If multiple logical partitions are sharing an Internet connection, you will need the IP addresses or host names created for TCP/IP and for virtual Ethernet.
2. For a dial-up (modem) connection, determine necessary configuration settings, including:
 - Local area code
 - Predial information, such as dialing 9 to dial outside the network
 - Use of commas if delayed dialing is needed
 - Any special telephone line conditions such as pulse (rotary) dialing or no dialtone.
 3. Ensure that TCP/IP is set up and configured correctly. If not, contact the network administrator and consult your operating system documentation.

Related concepts

“IP Packet Filter Firewall” on page 114

Learn how an IP packet filter firewall allows you to create a set of rules that either discard or accept traffic over a network connection.

Task 4. Ensure that your physical networking is set up correctly:

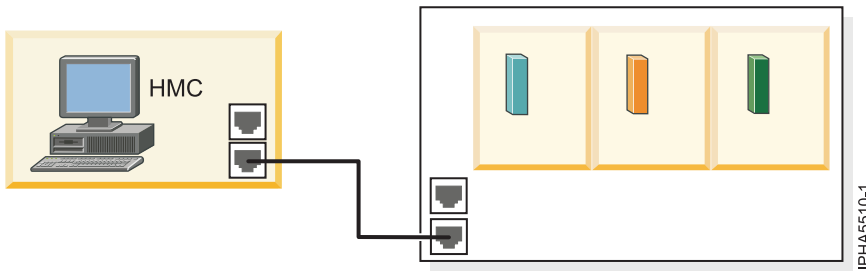
The underlying framework of your service environment is networking. The following networking connections are required for you to be able to take advantage of electronic services such as reporting hardware problems and other server information and downloading updates:

- Between the service processor and the HMC
- Between the HMC and the server (AIX and Linux)
- Between your site and service and support

1. Verify the physical connection between the service processor and the HMC.

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. 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:

Figure 36. This diagram shows the Ethernet connection between your HMC and the service processor on your server.



2. Verify the physical connection between the HMC and the server (AIX and Linux).

This connection allows your server to communicate with your HMC.

How you set up this connection depends on your configuration:

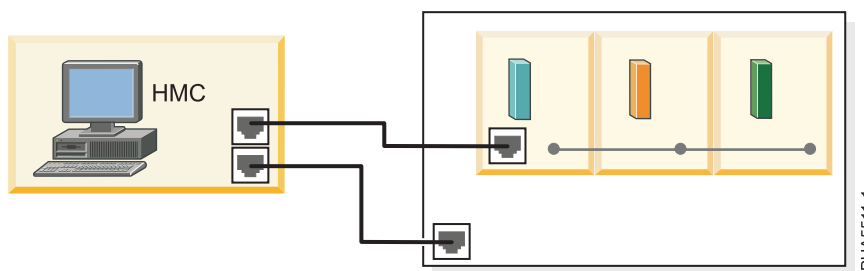
- If your server is in its manufacturing default configuration, you will make this connection when you set up your server.
- If your server has multiple logical partitions, you must ensure that your HMC can communicate with each logical partition and that the logical partitions can communicate with each 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 logical partitions. For instructions on how to configure TCP/IP, see your operating system documentation.

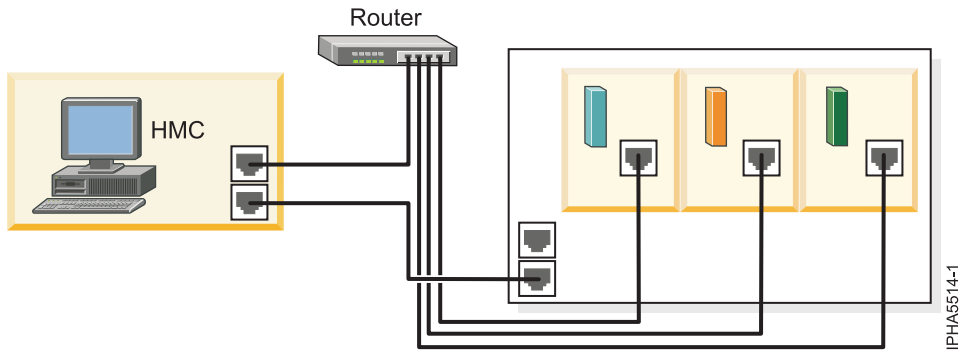
- Have an Ethernet adapter for one logical partition, most likely your service partition, and then use virtual Ethernet to enable the logical partitions to communicate with each other and with the HMC. This option is the preferred option because it requires that you have only one physical adapter in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

Figure 37. This diagram shows the Virtual Ethernet connection between your logical partitions and the physical Ethernet connection between your service partition and the HMC.



- 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:

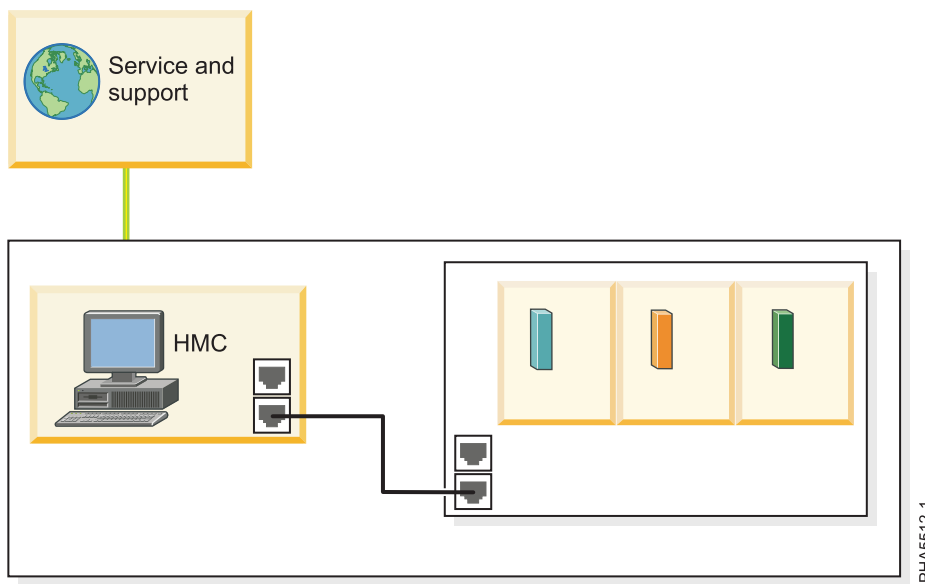
Figure 38. This diagram shows physical Ethernet connections between your logical partitions and your HMC through a router.



3. Verify the physical connection from your site to service and support.

This connection enables you to report hardware problems and other server information to service and support. It also enables you to install updates. This connection is represented in the following illustration:

Figure 39. This diagram shows the connection between service and support and a company that has a server and an HMC.



Task 5. Obtain or verify an IBM ID:

You will need an IBM ID to register IBM Electronic Service Agent on the HMC and for Electronic Service Agent on your operating system or systems. You also will need this ID to view information that has been reported to IBM through Electronic Service Agent.

1. Go to the My IBM Profile Web site.
2. Verify that you are registered.
 - If you are registered, Welcome back will be displayed on the Web site. Or, you can select **Sign in** and see if your e-mail address is recognized.
 - If you are not registered, select **Register** and fill out the registration form. Create an IBM ID for each of the people you want to have access to the information that Electronic Service Agent reports to IBM. You must associate these accounts with a server, usually your central server. (You can add other servers later.) The people for whom you create IDs must have system administrator authority on all registered servers.

3. Record your IBM ID (the e-mail address that you registered).
4. You will need the ID during “Task 6. Verify the HMC service settings using the Guided Setup wizard.”

Related information

 [My IBM Profile Web site](#)

Task 6. Verify the HMC service settings using the Guided Setup wizard:

To verify that the HMC service settings are set up correctly, use the Guided Setup wizard.

Note: If you have not set up your server, do that now. For details, refer to Initial server setup.

1. If you do not have an HMC, continue with “Task 8. Install the operating systems on your server or logical partitions” on page 90.
2. Access the Guided Setup wizard using the HMC interface:
 - a. In the navigation area, select the HMC that you want to work with.
 - b. Click **Information Center and Setup Wizard**.
 - c. In the contents pane, click **Launch the Guided Setup Wizard**. 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.
3. Click **Next** to skip the tasks that are not specific to setting up service, including:
 - 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
4. Ensure that the following service tasks are completed correctly:
 - a. Customer contact information for service-related activities, including:
 - Company name
 - Administrator name
 - E-mail address
 - Telephone numbers
 - Information regarding the location of the HMC
 - b. Configuration of connectivity for service-related activities.
 - **Internet VPN**

Note: When configuring the HMC’s network settings for connecting using direct or indirect Internet, the HMC must be configured with a default gateway to access the Internet. Select **HMC Management > HMC Configuration > Customize Network Settings**. Ensure that the Default Gateway Information field has a Gateway address listed and a selection is made in the Gateway device field (for example, any).

- **Internet:** Currently, the SSL option must be configured manually:
 - 1) Select **Service Applications → Remote Support → Customize Outbound Connectivity**
 - 2) Select the **Internet** tab.
- **Dial-up connection from the local HMC**
- **Connecting through other systems or logical partitions**
- c. Configuration of the network settings.
 - For direct or indirect Internet:
 - HMC host name
 - Domain name

- Description of HMC
 - For a dial-up modem connection:
 - Dial prefix, if applicable
 - Modem configuration, including:
 - Dial type
 - Dial prefix, if applicable
 - Telephone number
 - d. Authorize two users for Electronic Service Agent by entering the ID (the e-mail address that you registered with the My Profile Web site at <https://www.ibm.com/account/profile>).
- Note:** You will be able to authorize more users later.
- e. Add e-mail addresses for those you want to be notified when problem events occur.
5. To test the connection from the HMC, open **Service Applications** → **Remote Support** → **Customize Outbound Connectivity**.
 6. Select the tab for the type of outbound connectivity that you chose for your HMC (Local Modem, Internet, Internet VPN, or Pass-Through Systems). For more information about these settings, see Choosing your connection method.
 7. Click **Test**.
 8. Choose from the following options:
 - If the test is successful, continue with the next Task.
 - If the test fails, continue with the next step.
 9. Ensure that your country or region is listed. Select **Service Applications** → **Remote Support** → **Customize Customer Information**. Ensure that your country or region is selected from the list.
 10. Choose from the following options:
 - If you have a dial-up connection, perform the following:
 - Check the telephone line going into the HMC and the wall socket.
 - Check to make sure that you have the telephone number configured correctly, including predial information, such as dialing 9 to dial outside the network.
 - If you have an Internet VPN connection, perform the following:
 - Ensure that the appropriate firewall rules have been added, if necessary.
 - Check that you have a default gateway set up on the HMC. Select **HMC Management** → **HMC Configuration** → **Customize Network Settings**. Ensure that the Default Gateway Information field has a Gateway address listed and a selection is made in the Gateway device field (for example, any).

Related concepts

“Choosing your connection method” on page 4

Learn about choosing your connection method.

Related information

Initial server setup

Task 7. Set up and configure your logical partitions:

For details, refer to Partitioning the server.

Related information

Partitioning the server

Task 8. Install the operating systems on your server or logical partitions:

For details, refer to Installing operating systems.

Related information

Installing operating systems

Task 9. Configure your TCP/IP network:

For instructions, refer to the operating system documentation.

Task 10. Activate TCP/IP on your server or logical partitions:

Choose from the following options:

- If you are using AIX or Linux:
TCP/IP starts automatically, as long as the network adapter is recognized and can communicate with the network when the AIX or Linux operating system is started.
- If you are using i5/OS:
TCP/IP starts automatically, as long as the network adapter is recognized and can communicate with the network when the i5/OS operating system is started. If this does not occur, type STRTCP at an i5/OS command line to start TCP/IP. This command initializes and activates TCP/IP processing, starts the TCP/IP interfaces, and starts the server jobs. Only TCP/IP interfaces and servers with AUTOSTART *YES are started with the STRTCP command.

Task 11. Obtain and configure Electronic Service Agent for AIX or Linux:

If you have an HMC, you do not need to obtain and configure Electronic Service Agent for AIX or Linux. The AIX and Linux inventory and hardware-problem information (or report, perhaps) are sent through the HMC. However, you might want to set up Electronic Service Agent on AIX or Linux to contact the software service organization.

1. Choose from the following options:
 - If you have an HMC and do *not* want to obtain and configure Electronic Service Agent for AIX or Linux, continue with “Task 11.3. Configure the service processor (AIX and Linux)” on page 94.
 - If you want to obtain and configure Electronic Service Agent for AIX or Linux, continue with the next step.
2. Obtain Electronic Service Agent.
 - a. Go to the Electronic Service Agent Web site.
 - b. Follow the on-screen prompts to locate the instructions to obtain Electronic Service Agent.
3. Choose from the following options:
 - To configure Electronic Service Agent for AIX, continue with step 4.
 - To configure Electronic Service Agent for Linux, continue with step 9 on page 92.
4. To configure Electronic Service Agent for AIX, review the following information:

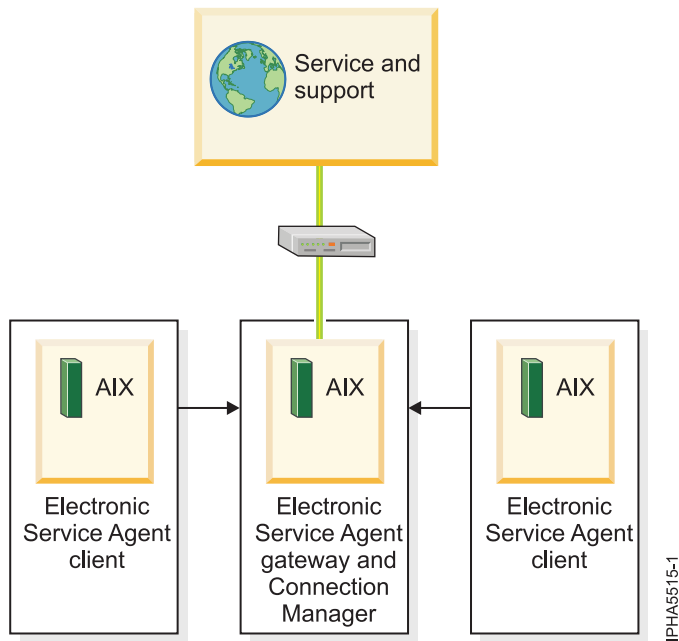
In this example, you will configure the following:

 - Electronic Service Agent on the server that has a modem for dial-up connection to service and support

Note: Alternatively, you can use an Internet or Secure Sockets Layer (SSL) connection instead of the modem to connect to service and support.

 - Electronic Service Agent on the other clients to communicate with the server that has the modem

Figure 40. This diagram shows three servers and their connection through a modem to service and support.



Note: For complex network environments involving HTTP proxies, SOCKS proxies, or DMZs, refer to the *Electronic Service Agent for IBM pSeries and IBM RS/6000 User's Guide*.

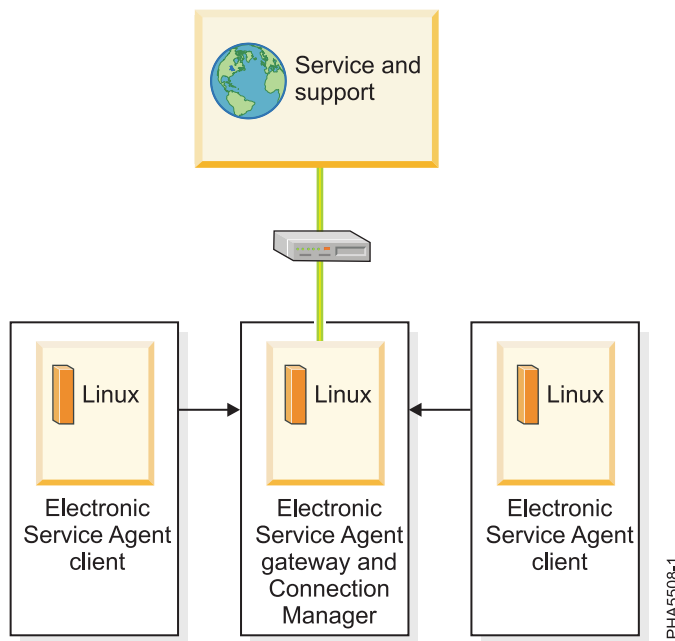
5. From the System Management Interface Tool (SMIT), configure and start Service Agent Connection Manager (SACM). The SACM is responsible for establishing connectivity to service and support. It enables the gateway server and clients to use a single, secure connection.

Note: More details on SMIT, see System Management Interface Tool SMIT.

- a. Verify that the host name for the SACM is correct. In this example, the SACM is located 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.
 - b. Verify the default port 1198. In most cases, the default port is appropriate. You can change the port later, if necessary. This port is necessary for communication between the gateway server and the SACM.
6. Configure and start the Electronic Service Agent gateway server. This is the server or logical partition that acts as the central management server for all of the clients (monitored servers or logical partitions). The Service Agent gateway server contains the central database, and it initiates communication to service and support. The Service Agent gateway communicates to service and support through the SACM.
 - a. Verify that the host name is correct. In this example, the SACM and SA gateway server are located on the same server. It is the server or logical partition with the modem. 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.
 - b. Verify that the machine type, model, and serial number are correct.
 7. Configure and start the Electronic Service Agent client. This is the monitored server or logical partition for which system information is collected and reported to service and support.
 - a. Verify that the host names for the SA clients and for the SA gateway are correct.
 - b. Verify that the machine type, model, and serial number are correct.
 8. Continue with "Task 11.1. Use the Service Agent (SA) Basic User Interface for AIX and Linux" on page 93.
 9. To configure Electronic Service Agent for Linux, review the following information.
In this example, you will configure the following:

- Electronic Service Agent on the server that has a modem for dial-up connection to service and support
- Note:** Alternatively, you can use an Internet or Secure Sockets Layer (SSL) connection instead of the modem to connect to service and support.
- Electronic Service Agent on the other clients to communicate with the server that has the modem

Figure 41. This diagram shows three servers and their connection through a modem to service and support.



- From the Linux command line, type the following command to configure and start Service Agent Connection Manager (SACM):

```
startsrc -s sacm
```

The SACM application enables the gateway server and client servers to use a single, secure connection to reach service and support.

- From the Linux command line, type the following command to configure and start the Electronic Service Agent gateway server:

```
/usr/svcagent/bin/sagatewayconfig
```

The Service Agent gateway server acts as the central management server for all of the clients (monitored servers or logical partitions). It contains the central database and initiates communication to service and support.

- Continue with "Task 11.1. Use the Service Agent (SA) Basic User Interface for AIX and Linux."

Related information

- [Electronic Service Agent Web site](#)
- [System Management Interface Tool SMIT](#)

Task 11.1. Use the Service Agent (SA) Basic User Interface for AIX and Linux:

You will need to install Electronic Service Agent on AIX or Linux to access the SA Basic User Interface. For details, refer to the Electronic Service Agent Web site and search for the appropriate Electronic Service Agent user's guide.

1. Get familiar with the SA 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.
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 guides you through the appropriate properties. For example, if you specify that you want to use a modem in the Connection Manager 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 or Linux and you use a modem for outbound connectivity, you need to complete specific information for the following properties:

ConnectionManager

Clear **False** for **Connect to SDR using Dialer** to enable the dialer. This indicates that you want to use a modem to connect to service and support.

Dialer Specify details about your modem and service and support connection parameters.

Machines

Add two SA client servers.

Enroll Register the servers with service and support. This initiates a call to service and support to enroll the servers in service and support's database. To complete the process, service and support sends you a key.

Call log

Check the status of the call to service and support. You can see whether the call to service and support is successful.

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.

Related information



Electronic Service Agent Web site

Task 11.2. Register the ID with Service Agent for AIX or Linux:

1. From the Service Agent Basic User Interface, click **Enroll**.
2. Complete the required fields on the right side of the interface. Required fields are indicated with an exclamation point.
3. Continue with "Task 11.3. Configure the service processor (AIX and Linux)."

Task 11.3. Configure the service processor (AIX and Linux):

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.

Note: If you are using a 7037-A50 or 7047-185 server, this task does not apply. Continue with "Task 13. Test the connection to service and support" on page 100.

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

Note: For i5/OS, it is not necessary to configure the service processor to call service and support because this is handled by the i5/OS operating system.

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.

Note: To perform these tasks, you must have an authority level of either Administrator or Service provider.

2. In the navigation area, expand **System Service Aids**.
3. To configure the service processor system port, follow these steps:
 - a. Select **Serial Port Setup**.
 - b. Modify the appropriate fields in the S1 (used with the call-home feature) and S2 (used with the call-in feature) sections.
 - c. Click **Save settings** to save the setting changes.
4. To configure the modem, follow these steps:
 - a. Select **Modem Configuration**.
 - b. Modify the appropriate fields in the S1 and S2 sections.
 - c. Click **Save settings**.
5. To configure the call-home and call-in policy, follow these steps:
 - a. Select **Call-in/Call-home**.
 - b. Enter the desired text into the specified fields.
 - c. Click **Save settings** to save changes.
6. To test the call-home policy, follow these steps:
 - a. Select **Call-Home Test**.
 - b. Click **Initiate call-home test**. A test of the call-home system is performed as specified by the current port and modem selections.
7. Continue with "Task 13. Test the connection to service and support" on page 100.

Task 12. Configure Electronic Service Agent for i5/OS:

1. Ensure that the following software is installed (use the DSPSFWRSC command to confirm).

Note: Electronic Service Agent and the following software is included with the base i5/OS operating system starting with V5R3.

- 5722SS1 – Option 34 (OS/400 - Digital Certificate Manager)
- If you have i5/OS V5R3, you will need 5722AC3 (Cryptographic Access Provider 128-bit). This is a security provision to encrypt communications between your system and service and support.

Note: The 5722AC3 (Cryptographic Access Provider 128-bit) is not necessary starting with i5/OS V5R4.

- 5722JC1 (IBM Toolbox Kit for Java)
2. At the command line, type G0 SERVICE. One of the following occurs:
 - If connectivity was set up previously, type 18 to get to the configuration menu where you can create, change, delete, or verify that connectivity works. If you want to change the settings, continue with step 3.
 - If connectivity has never been set up on this logical partition or server, the system will try to ping one of the IBM gateways. If this is successful, the interface will prompt for configuring direct Internet. If this is successful, the default settings for direct Internet will be prefilled. If you want to verify or change these default settings, continue with step 3.

Note: In some environments, the pinging of the IBM gateway does not work because the firewall might be blocking the packets. However, you should still verify with the network administrator if the criteria is met to set up direct Internet. For details, see "Task 3. Prerequisites" on page 85.

3. Choose from the following options:
 - To set up a direct Internet connection from each i5/OS server or logical partition, go to step 4 on page 96.

- To set up a shared direct Internet connection, go to step 6.
 - To set up a modem or shared modem connection, go to step 11 on page 98.
 - To set up a connection through the modem on the HMC, go to step 17 on page 99.
4. To set up a direct Internet connection from each i5/OS server or logical partition, specify the following information from each logical partition in the CRTSRVCFG prompts:

For i5/OS V5R3:

- Connection type: *VPN
- Virtual private network type: *DIRECT
- Connectivity for others: Connect point: *NO

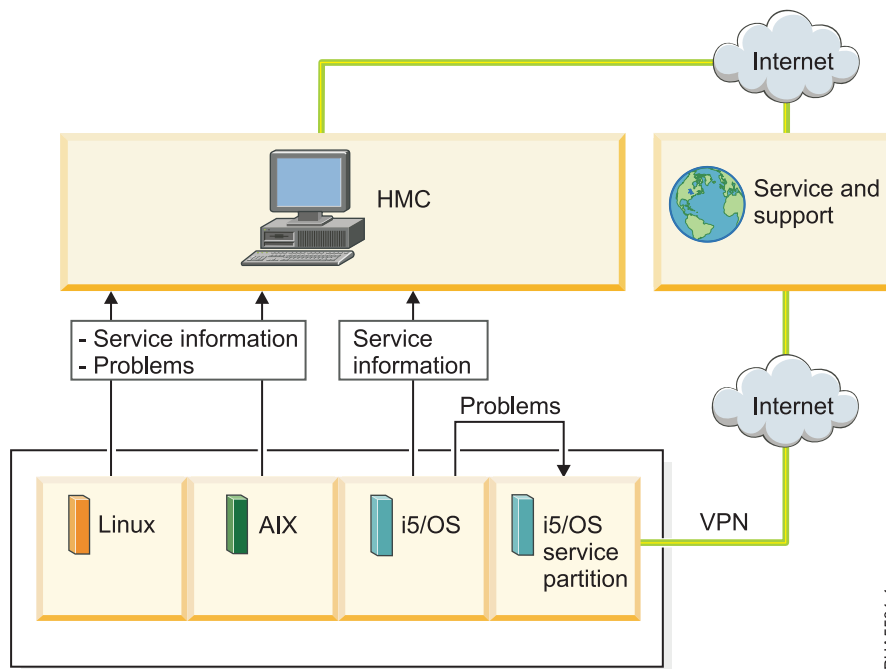
For i5/OS V5R4:

- Role: *PRIMARY
- Connection type: *DIRECT
- Connectivity for others: Connect point: *NO

Note: For additional details on using Electronic Service Agent, refer to the Electronic Service Agent topic in the iSeries Information Center.

5. Continue with “Task 12.1 Register the IBM ID for i5/OS” on page 100.
6. To set up a shared direct Internet connection, review the following information.
- A direct Internet connection from the i5/OS logical partition that has connectivity to the Internet.
 - Enable the other logical partitions to connect to the logical partition that has connectivity to the Internet

Figure 42. This diagram shows the flow of information and problems from four logical partitions and the HMC to service and support. The service information passes through the HMC to service and support over a direct Internet connection. And, problems from i5/OS pass through the i5/OS logical partition to service and support.



7. Specify the following information from the i5/OS server or logical partition with Internet connectivity in the CRTSRVCFG prompts:

For i5/OS V5R3:

- Connection type: *VPN
- Virtual private network type: *DIRECT
- Connectivity for others:
 - Connect point: *YES. This enables other logical partitions or systems to use the VPN connection on this logical partition to connect to service and support.

Note: You will need to create service configurations on the remote systems or logical partitions that will be using this connection point.

- Interfaces: *ALL or a list of the interfaces over which you will accept connections to service and support.

For i5/OS V5R4:

- Role: *PRIMARY
- Connection type: *DIRECT
- Connectivity for others:
 - Connect point: *YES. This enables other logical partitions or systems to use the VPN or service and support proxy connection on this logical partition to connect to service and support.

Note: Service configurations need to be created on the remote systems or logical partitions that will be using this connection point.

- Interfaces: *ALL or a list of the interfaces over which you will accept connections to service and support.

8. Specify the following information from each of the other i5/OS server or logical partitions in the CRTSRVCFG prompts:

For V5R3 i5/OS:

- Connection type: *VPN
- Virtual private network type: *MULTIHOP
- Remote system: Enter the host name or IP address of the logical partition with the Internet connectivity.

Note: A multi-hop VPN connection from an i5/OS system or logical partition using the IP address of the HMC is not supported. The only connectivity option for an i5/OS logical partition to the HMC is to use a remote PTP configuration.

- Connectivity for others: Connect point: *NO

For i5/OS V5R4:

- Connection type: *MULTIHOP
- Remote system: Enter the host name or IP address of the logical partition with the Internet connectivity.

Note: A multi-hop VPN connection from an i5/OS system or logical partition using the IP address of the HMC is not supported. The only connectivity option for an i5/OS logical partition to the HMC is to use a remote PTP configuration.

- Proxy server: Enter the information about the Service and Support Proxy (or your own HTTP proxy) as follows:
 - IP address or host name: Enter the host name or IP address of the logical partition with the Internet connectivity (or if you have your own HTTP proxy, you could also specify that).
 - Port number: Enter the port number of the Service and Support proxy or your own HTTP proxy. Default of *IBMSVR which is 5026 (the default for the Service and Support proxy).
 - Relative priority: Enter the priority (relative to the multi-hop VPN)
- Connectivity for others: Connect point: *NO

9. Verify that interpartition communication is set up. Ping the host or IP address of the logical partition that has the Internet connectivity or modem from the logical partition that needs to use the Internet connection or modem.

Note: For additional details on using Electronic Service Agent, refer to the Electronic Service Agent topic in the iSeries Information Center.

10. Continue with “Task 12.1 Register the IBM ID for i5/OS” on page 100.
11. To set up a modem or shared modem on your i5/OS server or logical partition, choose from the following options:
 - To set up a modem from an i5/OS server, go to step 12.
 - To set up a shared modem, go to step 14.
12. To set up a modem from an i5/OS server or logical partition, specify the following options from the server in the CRTSRVCFG prompts:

For i5/OS V5R3:

 - Connection type: *PTP
 - Virtual private network type: *LOCAL
 - Service: *SRVAGT

For i5/OS V5R4:

 - Connection type: *LCLDIAL
 - Connectivity for others: Connect point: *NO

Note: For additional details on using Electronic Service Agent, refer to the Electronic Service Agent topic in the iSeries Information Center.

13. Continue with “Task 12.1 Register the IBM ID for i5/OS” on page 100.
14. To set up a shared modem (you have multiple systems or logical partitions), specify the following information from the system or logical partition with the modem in the CRTSRVCFG prompts:

For i5/OS V5R3:

 - Connection type: *PTP
 - Virtual private network type: *LOCAL
 - Service: *SRVAGT
 - Connectivity for others:
 - Connect point: *YES: This enables other logical partitions or systems to use the PTP dial connection on this logical partition to connect to service and support.

Note: Service configurations need to be created on the remote systems or logical partitions that will be using this connection point.

- Interfaces: *ALL or a list of the interfaces over which you will accept connections to service and support.

For i5/OS V5R4:

- Connection type: *LCLDIAL
- Connectivity for others:
 - Connect point: *YES: This enables other logical partitions or systems to use the dial connection on this logical partition to connect to service and support.

Note: Service configurations need to be created on the remote systems or logical partitions that will be using this connection point.

- Interfaces: *ALL or a list of the interfaces over which you will accept connections to service and support.

15. Specify the following information from each of the other i5/OS servers or logical partitions in the CRTSRVCFG prompts:

For i5/OS V5R3:

- Connection type: *PTP
- Point to point type: *REMOTE
- Service: *SRVAGT
- Remote system: Enter the host name or IP address of the system or logical partition with the modem.

For i5/OS V5R4:

- Connection type: *RMTDIAL
- Remote system: Enter the host name or IP address of the system or logical partition with the modem.

Note: For additional details on using Electronic Service Agent, refer to the Electronic Service Agent topic in the iSeries Information Center.

16. Continue with “Task 12.1 Register the IBM ID for i5/OS” on page 100.
17. To set up a connection from an i5/OS server or logical partition through the HMC’s modem, specify the following information in the CRTSRVCFG prompts from each logical partition that will use the HMC’s modem:

For i5/OS V5R3:

- Connection type: *PTP
- Point to point type: *REMOTE
- Service: *SRVAGT
- Remote system: Enter the IP address or host name of the interface on the HMC through which you will connect to service and support.

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, continue with the next step.

For i5/OS V5R4:

- Connection type: *RMTDIAL
- Remote system: Enter the IP address or host name of the interface on the HMC through which you will connect to service and support.

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, continue with the next step.


18. To find the interface that provides partition communication, follow these steps from the HMC interface:
 - a. In the navigation area, expand the HMC you want to work with. The HMCs are listed by host name or IP address.
 - b. Expand **HMC Management**.
 - c. Click **HMC Configuration**.
 - d. In the contents pane, click **Customize network settings**.
 - e. Click the **LAN Adapters** tab.
 - f. Select a LAN adapter and click **Details**.

- g. Click the **Lan Adapter** tab. In the Local Area Network Information section, the Partition communication checkbox indicates whether this interface is used for partition communication.

Note: For additional details on using Electronic Service Agent, refer to the Electronic Service Agent topic in the iSeries Information Center.

19. Continue with "Task 12.1 Register the IBM ID for i5/OS."

Related information

 Electronic Service Agent in the iSeries Information Center

Task 12.1 Register the IBM ID for i5/OS:

Register the IBM ID with Electronic Service Agent for i5/OS by following these steps:

1. At the i5/OS command line, type `GO SERVICE`.
2. From the Electronic Service Agent menu, select **Authorize users to access service information** and press Enter.
3. Type your IBM ID (internet address that you registered with the My Profile Web site at <https://www.ibm.com/account/profile>) in the Authorize users field and press Enter.
4. Continue with "Task 13. Test the connection to service and support."

Task 13. Test the connection to service and support:

1. If you use an HMC to connect to service and support, follow these steps to test the connection for the HMC:
 - a. On the HMC, open **Service Applications > Service Focal Point > Service Utilities**.
 - b. Select a system.
 - c. Select **Selected > Create serviceable event**.
 - d. Select **Test automatic problem reporting**.
 - e. Select **Request Service**. A message is displayed when the service request is sent.
2. To test the connection for AIX (if you set up Electronic Service Agent on the server or logical partition), follow these steps:
 - a. From the System Management Interface Tool (SMIT) on your Electronic Service Agent server, activate the Electronic Service Agent.
 - b. Ensure that the Electronic Service Agent Connection Manager is active if it is located on a machine other than the Electronic Service Agent server.
 - c. From SMIT, start the Service Agent Advanced User Interface.
 - d. To use a modem, follow the instructions to configure the dialer on the Connection Manager screen. The default is to connect to service and support using an existing Internet connection.
 - e. Open the **Manual Tools** folder.
 - f. Select **Connect**.
 - g. Monitor the CallLog for the following entry: TEST Connection (Success: 1, Fail: 0).
3. To test the connection for i5/OS servers or logical partitions, perform the following steps.
 - a. To test the Electronic Service Agent connection, enter the following command at the command line:
`GO SERVICE`
 - b. From the Electronic Service Agent menu, select option 17 (Verify Service Configuration), and press Enter. A message is displayed that indicates whether the test connection is successful.
 - c. To test the electronic customer support connection profile, enter the following command:
`SNDSRVRQS *TEST`

A message is displayed that indicates whether the test connection is successful.

4. To test the connection for Linux (if you set up Electronic Service Agent on the server or logical partition), follow these steps:
 - a. On your Electronic Service Agent server, activate the Electronic Service Agent.
 - b. At a Linux command line, type the following:
`startsrc -g svcagent`
 - c. Ensure that the Electronic Service Agent Connection Manager is active if it is located on a machine other than the Electronic Service Agent server.
 - d. At a Linux command line, type the following:
`startsrc -s sacm`
 - e. Start the Service Agent Advanced User Interface.
 - f. At a Linux command line, type the following:
`/usr/svcagent/bin/sauiascii`
 - g. If you want to use a modem, follow the instructions to configure the dialer on the Connection Manager screen. The default is to connect to service and support using an existing Internet connection.
 - h. Open the **Manual Tools** folder.
 - i. Click **Connection**.
 - j. Monitor the CallLog for the following entry: TEST Connection (Success: 1, Fail: 0).

Task 14. View the server information that was reported:

You can use the Internet to view details of the system you have enabled, and see the data collected by Electronic Service Agent. To use the advanced features and receive the full benefits of Electronic Service Agent, you must enter an IBM Registration ID (IBM ID). The first IBM ID entered will have Administrator authority and is able to authorize additional users on the Web site. The second IBM ID is available as a backup for the Administrator.

1. Go to the IBM Electronic Services Web site.
2. Click **Sign in** (in the upper-right corner).
3. Type the IBM ID and password.
4. Choose the following options from the navigation bar:
 - To view your server information, click **My systems**.
 - To search technical support using your server information to improve the search results, click **Premium Search**.

Note: In some cases, the Premium Search feature is available only while your server is under warranty or afterward through a service contract.

- To view information related to your servers and interests, click **My messages**.
5. Enter the requested information.

Related information

 [Electronic Service Agent Web site](#)

Ensuring security when using Electronic Service Agent

Learn about the various security features when you are connected to IBM service and support using Electronic Service Agent.

IBM Electronic Service Agent is a software application that is used for collecting and transporting machine information to IBM's service and support organization. The information collected is for problem analysis, periodic checking, and inventory reporting. The information collected by Electronic Service Agent helps provide you with faster problem identification and resolution.

Transmission security

The transmission of Electronic Service Agent information is performed by a security-rich process. Depending on the connection options available, the transaction is by modem or in many networks, using direct Internet. Allowing access between the Internet and your network raises security and privacy concerns. IBM has taken the steps necessary to provide security-enhanced transmissions for Electronic Service Agent transactions.

Connection options

There are several connection options for Electronic Service Agent at this time, and the platform User Guide will provide the most current listing. A few of the most common connection options are:

Modem

IBM Electronic Service Agent uses the AT&T Global Network Services (AGNS) dialer for modem access. Electronic Service Agent provides AGNS ID and password electronically, in the background. You will not be able to view this information. This is an exclusive account for Electronic Service Agent. No incoming calls are allowed to the modem.

Internet HTTPS

IBM Electronic Service Agent uses HTTPS, which utilizes SSL 128-bit encryption and TCP/IP protocols. Electronic Service Agent might be configured to work with firewalls and authentication proxies. The Internet provider relationship and connection are customer responsibilities.

Internet virtual private network (VPN)

A VPN gives users the privacy of a separate network over public lines by substituting encryption and other security measures for the physically separate network lines of traditional private networks. VPNs require configuration of an access device, either hardware-based or software-based. In the case of Electronic Service Agent there are several software programs utilized when creating a VPN.

Privacy of client information

The inventory information that is gathered from your systems is information typically collected verbally from you during telephone calls with the IBM support center, pre-sales specialists, administrative clerks and other groups within IBM that work with you to provide the best possible service (technical or administrative). These IBM groups will have electronic access to the information so that they can prepare for service, do advanced problem determination, and more efficiently serve you.

Enable remote support

Learn how to set up your server so that you can enable remote support centers to connect and manage your server or your HMC after you permit it.

Remote support enables you to securely give the service and support organization access to your HMC or server to enable problem analysis and determination.

Remote support methods

Use this information to learn about the remote support methods that are available to you.

If you are using your server with an HMC, you can use the following communication methods to enable this connection:

Direct Internet, including Virtual private networking (VPN) or a Secure Sockets Layer (SSL connection)

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.

Enabling remote support on the HMC

Use this information to learn how to allow the service and support organization to access your server or HMC.

To enable remote service representatives 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 the service and support organization. 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

Use this information to learn how to enable remote support when you do not have an HMC.

Enabling remote support without an HMC when you have AIX or Linux:

Use this information to learn how to enable remote support when you do not have an HMC and you have AIX or Linux.

If your server is in its manufacturing default configuration, you can still enable service representatives to do problem determination.

If you have AIX or Linux installed on your server, you can enable the service and support organization 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 "Task 12. Configure the service processor" in Setting up AIX or Linux to connect to service and support without an HMC.

Related tasks

"Task 12. Configure the service processor" on page 64

Related information

Partitioning the server

Enabling remote support without an HMC when you have i5/OS.:

Use this information to learn how to enable remote support when you do not have an HMC when you have i5/OS.

If your server is in its manufacturing default configuration, you can still enable service representatives to do problem determination.

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

Partitioning the server



Electronic Service Agent in the iSeries Information Center

Supporting information for setting up your service environment

Find additional information about setting up connectivity to service and support.

Requirements needed by service personnel

Learn about the requirements that the service personnel need to have available when they service your systems.

IBM requires that the customer provide the following for the service representative's use:

- A supported HMC, a system console, a PC capable of connecting to the ASMI , or any combination of these needed by the service representative in order to service your system.
- All current, supported software, installed on the devices and correctly configured, with current software fixes applied.
- Consoles in the same room and within 8 meters (26 feet) of the system being serviced.
- Devices that are connected to the system, are operating, and are communicating with the system prior to the arrival of the service representative.
- Be available to enter passwords that are needed by service personnel to access and repair your system. For example, the ASMI, HMC, or operating system.

Delays to service representatives that are caused by a failure to meet the preceding requirements are billable at current hourly rates.

Note: The HMC or system console might be capable of providing the required ASMI connection, if configured.

Manually set up the HMC to connect to service and support

Learn the steps to manually set up the HMC if you do not want to use the HMC Wizard.

Use this procedure if you do not want to use the HMC Guided Setup wizard to set up your HMC to connect to service and support. The following steps are required to set up service connectivity from the HMC to service and support:

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

1. Set up networking for your service environment. For details, see Networking for your service environment.
2. Specify the connection method. For details, see Specifying the connection type from the HMC.
3. Specify your company's contact and account information. For details, see Specifying your company's contact and account information.
4. Configure the Electronic Service Agent on your HMC. For details, see Configuring Electronic Service Agent on your HMC.
5. Specify the options that enable Electronic Service Agent and Service Focal Point to perform service tasks. For details, see Specifying options for connection monitoring.

Related concepts

“Configuring Electronic Service Agent on your HMC” on page 108

Learn how to configure Electronic Service Agent on your HMC.

Related tasks

“Networking for your service environment”

Learn about the networking options for your service environment.

“Specifying the connection type from the HMC” on page 107

Learn how to specify the connection type from the HMC.

“Specifying your company’s contact and account information” on page 108

It is important that you specify contact and account information on the HMC because it helps the service and support organization contact the correct person in your company in the event of a system problem.

“Specifying options for connection monitoring” on page 112

Learn how to change the options you use for watching the communication paths between your HMC and its managed systems.

Supporting information for connecting the HMC to service and support

Learn more about the options for configuring the HMC for connecting to the service and support organization.

Networking for your service environment:

Learn about the networking options 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 updates:

1. Verify the physical connection between the service processor and the HMC.

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. 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:

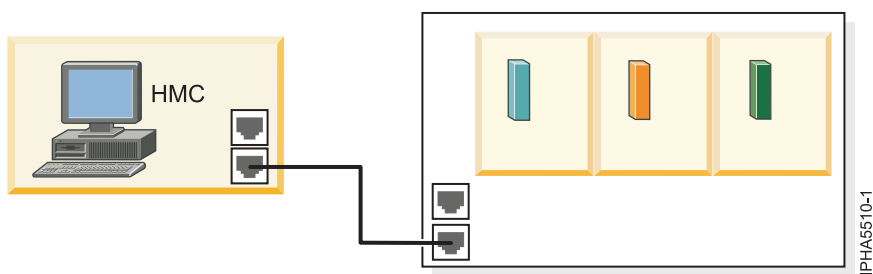


Figure 43. This diagram shows the Ethernet connection between your HMC and the service processor on your server.

2. Verify the physical connection between the HMC and the server (AIX and Linux).

This connection allows your server to communicate with your HMC.

How you set up this connection depends on your configuration:

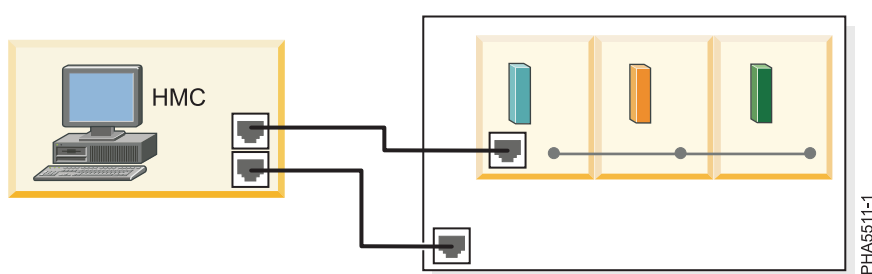
- If your server is in its manufacturing default configuration, you will make this connection when you set up your server.
- If your server has multiple logical partitions, you must ensure that your HMC can communicate with each logical partition and that the logical partitions can communicate with each 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 logical partitions. For instructions on how to configure TCP/IP, see your operating system documentation.

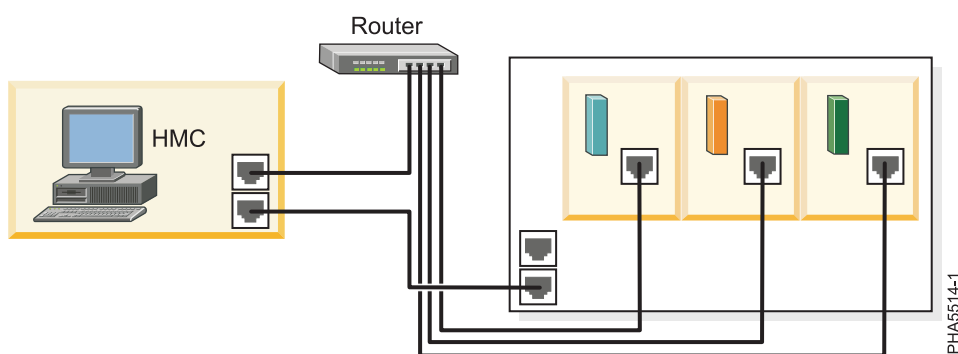
- Have an Ethernet adapter for one logical partition, most likely your service partition, and then use virtual Ethernet to enable the logical partitions to communicate with each other and with the HMC. This option is the preferred option because it requires that you have only one physical adapter in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

Figure 44. This diagram shows the Virtual Ethernet connection between your logical partitions and the physical Ethernet connection between your service partition and the HMC.



- 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:

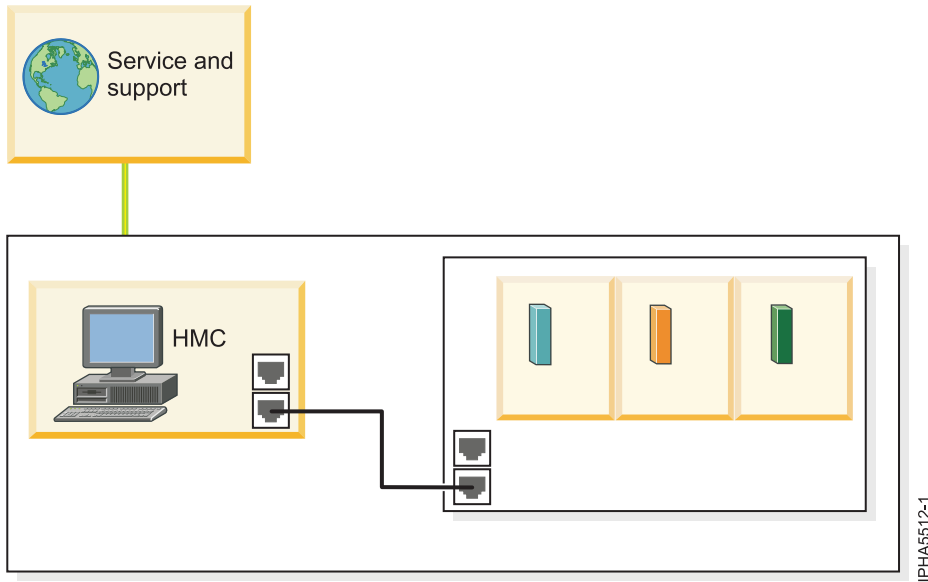
Figure 45. This diagram shows physical Ethernet connections between your logical partitions and your HMC through a router.



3. Verify the physical connection from your site to service and support.

This connection enables you to report hardware problems and other server information to service and support. It also enables you to install updates. This connection is represented in the following illustration:

Figure 46. This diagram shows the connection between service and support and a company that has a server and an HMC.



Specifying the connection type from the HMC:

Learn how to specify the connection type from the HMC.

To find out more about the connection types, see [Connectivity](#).

Use the Remote Support application on the HMC to specify which kind of connection you want to use. Follow these steps on your HMC:

1. In the navigation area, open **Service Applications**.
2. Select **Remote Support**.
3. Select **Customize Outbound Connectivity**.
4. Choose from the following options:

Local modem

This option enables you to send problem information and system data to service and support using the modem on your HMC. You can 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 service and support using a high-speed Internet connection on your HMC. 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.

Note: Internet and Internet VPN are both preferred options for connectivity because they can utilize an existing high-bandwidth internet connection which allows for enhanced service and support.

Internet

Allows you to enable the use of an existing Internet connection for outbound connectivity that allows the HMC to perform call-home functions over an encrypted Internet Secure Sockets Layer (SSL) connection.

Note: Internet and Internet VPN are both preferred options for connectivity because they can utilize an existing high-bandwidth internet connection which allows for enhanced service and support.

Pass-Through Systems

This option enables you to send problem information to service and support 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 they are the only logical partitions that can be used as pass-through systems.

You can 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 a direct Internet connection on an i5/OS logical partition.

Related concepts

“Choosing your connection method” on page 4
Learn about choosing your connection method.

Related tasks

“Scenario: Multiple AIX logical partitions with an HMC” on page 13
Learn how to connect your AIX logical partitions to enable service features on your server and your HMC.

“Scenario: Multiple IBM i5/OS logical partitions using the HMC’s modem” on page 20
Learn how to configure multiple logical partitions to connect to service and support through the modem on the HMC.

“Scenario: Multiple IBM i5/OS logical partitions using a direct Internet connection on an i5/OS logical partition” on page 18
Learn how to configure multiple logical partitions to connect to service and support through a direct Internet connection on an i5/OS logical partition.

Specifying your company’s contact and account information:

It is important that you specify contact and account information on the HMC because it helps the service and support organization contact the correct person in your company in the event of a system problem.

The contact and account information also can be used to gather information about your company’s service history, which might 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 from your HMC:

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

Configuring Electronic Service Agent on your HMC:

Learn how to configure Electronic Service Agent on your HMC.

You can use Electronic Service Agent on your HMC to share server information and hardware problem information with service and support 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 service and support 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

Specifying when and how Electronic Service Agent sends information to service and support:

Learn how to specify when and how Electronic Service Agent shares information with service and support.

Specifying the timetable for transmitting service information:

Use Electronic Service Agent to define the timetable on which you want to share service information with service and support.

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 system information to service and support immediately, click **Send**.
6. To schedule when and how often you send information to service and support, select **Schedule when to transmit the service information**, and specify the frequency and time.

Using File Transfer Protocol to send service information:

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

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:

Learn how you can be notified when hardware problems occur on your server.

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:

Setting up 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 service and support. 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 about 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 (<http://www.rfc-editor.org/rfcsearch.html>) .

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.

Related concepts

"SNMP traps"

Learn about creating programs that display or parse the information contained in an SNMP trap.

SNMP traps:

Learn about creating programs that display or parse the information contained in an SNMP trap.

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

enterprise specific (6)

Specific trap

3

Variable list

cpsSystemSendTrap

Description

Problem Log Entry Created

Generated when a problem is added to a problem log on a converged power system.

```
cpsSystemNotifyTrap='yyyy/MM/dd hh:mm:ss tzn\n
Manufacturer=IBM\n
ReportingMTMS=tttt-mmm*ppzzzz\n
ProbNm=nnnnn\n
LparName=lparname\n
FailingEnclosureMTMS=tttt-mmm*ppzzzz\n
SRC=ssssssss\n
EventText=79 char string\n
Fru1Info=71 char string\n
Fru2Info=71 char string\n
Fru3Info=71 char string\n
```

Where:

\n = RETURN

yyyy = year

MM = month

dd = day

hh = hour(24)

mm = minute

ss = seconds

tzn = time zone

tttt = type number (for example, 2107)

mmm = model number (for example, 921)

pp = plant of manufacture (for example, 75)

zzzzz = sequence number (for example, FA123)

nnnnn = problem number

lparname

= logical partition name

ssssssss

= system reference code

FruNInfo

= information about FRU N, where n is 1,2,3

Specifying options for connection monitoring:

Learn how to change the options you use for watching the communication paths between your HMC and its managed systems.

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 communications 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*.

Related concepts

“Configuring Electronic Service Agent on your HMC” on page 108
Learn how to configure Electronic Service Agent on your HMC.

Using IBM i5/OS applications and interfaces to set up connections to service and support

Learn more about the options for configuring the i5/OS for connecting to the service and support organization.

Using the Universal Connection wizard to connect IBM i5/OS to service and support:

Learn how you can use the Universal Connection wizard to connect i5/OS to service and support.

You can use the Universal Connection wizard in System i 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 System i Information Center.

Choose from the following options:

VPN

Modem on the server

Through the HMC

Connecting to service and support through a VPN connection using the Universal Connection wizard

If you choose to use the Universal Connection wizard to connect to service and support 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 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 multi-hop connection through a remote server scenario in the Universal Connection topic; perform these steps from each of the other logical partitions.

Connecting to service and support through the modem on the server using the Universal Connection wizard

If you choose to use the Universal Connection wizard to connect to service and support 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.

Connecting to service and support through the HMC using the Universal Connection wizard

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

Using the Extreme Support wizard to connect IBM i5/OS to service and support:

Learn how you can use the Extreme Support wizard to connect i5/OS to service and support.

You can use the Extreme Support wizard in System i 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 can configure the connection profiles with the Extreme Support wizard.

The Extreme Support wizard provides the following advantages:

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

Choose from the following options:

- VPN

- Modem on the server
- Through the HMC

Connecting to service and support through a VPN connection using the Extreme Support wizard

If you choose to use the Extreme Support wizard to connect to service and support 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 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 multi-hop connection through a remote server scenario in the Universal Connection topic; perform these steps from each of the other logical partitions.

Connecting to service and support through the modem on the server using the Extreme Support wizard

If you choose to use the Extreme Support wizard to connect to service and support 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.

Connecting to service and support through the HMC using the Extreme Support wizard

If you choose to use the Extreme Support wizard to connect to service and support 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.

Using IBM Performance Management for eServer iSeries:

Learn how you can use performance-trend analysis on i5/OS.

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

IP Packet Filter Firewall:

Learn how an IP packet filter firewall allows you to create a set of rules that either discard or accept traffic over a network connection.

An IP packet filter firewall allows you to create a set of rules that either discard or accept traffic over a network connection. The firewall itself does not affect this traffic in any way. Because a packet filter can only discard traffic that is sent to it, the device with the packet filter must either perform IP routing or be the destination for the traffic.

A packet filter has a set of rules with accept or deny actions. When the packet filter receives a packet of information, the filter compares the packet to your pre-configured rule set. At the first match, the packet filter either accepts or denies the packet of information. Most packet filters have an implicit "deny all rule" at the bottom of the rules file.

Packet filters usually permit or deny network traffic based on:

- Source and destination IP addresses
- Protocol, such as TCP, UDP, or ICMP
- Source and destination ports and ICMP types and codes
- Flags in the TCP header, such as whether the packet is a connect request
- Direction (inbound or outbound)
- Which physical interface the packet is traversing

All packet filters have a common situation: The trust is based on IP addresses. Although this security type is not sufficient for an entire network, this type of security is acceptable on a component level.

Most IP packet filters are stateless, which means they do not remember anything about the packets they previously processed. A packet filter with state can keep some information about previous traffic, which gives you the ability to configure that only replies to requests from the internal network are allowed from the Internet. Stateless packet filters are vulnerable to spoofing because the source IP address and ACK bit in the packet's header can be easily forged.

You can specify in i5/OS the packet filter rules on interfaces and remote access service profiles. If you are using either an external packet filter firewall or packet filter rules on the i5/OS and your Universal Connection data passes through these filters, you must change the filter rules to allow the connection to the IBM VPN Gateway as follows:

Table 1. IBM VPN Gateway filter rules

IP filter rules	IP filter values
UDP inbound traffic filter rule	Allow port 4500 for VPN gateway address
UDP inbound traffic filter rule	Allow port 500 for VPN gateway address
UDP outbound traffic filter rule	Allow port 4500 for VPN gateway IP address
UDP outbound traffic filter rule	Allow port 500 for VPN gateway IP address
ESP inbound traffic filter rule	Allow ESP protocol (X'32') for VPN gateway IP address
ESP outbound traffic filter rule	Allow ESP protocol (X'32') for VPN gateway IP address

For those Universal Connection applications that use HTTP and HTTPs for a transport, you must change the filter rules to allow connections to the IBM service destinations as follows:

Table 2. HTTP and HTTPs filter rules

IP filter rules	IP filter values
TCP inbound traffic filter rule	Allow port 80 for all service destination addresses
TCP inbound traffic filter rule	Allow port 443 for all service destination addresses
TCP outbound traffic filter rule	Allow port 80 for all service destination addresses
TCP outbound traffic filter rule	Allow port 443 for all service destination addresses

Changing the filter rules involves specifying the actual IBM VPN Gateway address. The ports and services must be opened for the following IPs: Boulder: 207.25.252.196 and Rochester: 129.42.160.16. For more details, see Determine the IBM VPN Gateway addresses in the iSeries Information Center.

In addition, for HTTP and HTTPs traffic, part of changing the filter rules might involve specifying actual service destination addresses. You can determine these addresses as described in Determine the IBM Service Destination addresses in the iSeries Information Center.

Updates

Learn about obtaining machine code updates for your HMC, server firmware, power subsystem firmware (if you have a model 575 or 59x server), I/O adapter and device, as well as operating system updates.

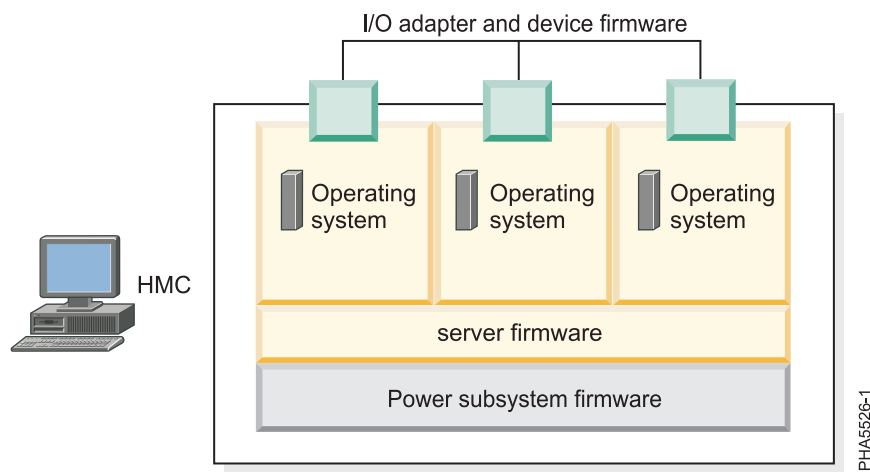
Updates provide changes to your software, Licensed Internal Code, or machine code that fix known problems, add new function, and keep your server or HMC operating efficiently. For example, you might install updates for your operating system in the form of a PTF (program temporary fix). Or, you might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

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

You can get updates 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 firmware updates. If you do not use an HMC to manage your server, you can use the functions specific to your operating system to get your updates. In addition, you can download or order many updates through Internet Web sites.

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

Figure 47. A diagram that shows the hardware and software that might require updates, including the HMC, I/O adapters and devices firmware, server firmware, power subsystem firmware, and operating systems.



Concepts for obtaining updates through the HMC

Learn about firmware levels, concurrent firmware updates, and the permanent and temporary side of the service processor.

Levels of firmware on the HMC

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

If you use an HMC to manage your server, you can use the HMC interface to view the levels of server firmware and power subsystem firmware that are installed on your server, and are available to download and install.

For information on recommended levels of system firmware and Hardware Management Console machine code, see the POWER5™ Code Matrix Web site.

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

Related information

 [POWER5 Code Matrix Web site](#)

Existing levels of server firmware and power subsystem firmware: The server has the following levels of server firmware and power subsystem firmware installed:

Installed level

This is the level of server firmware or power subsystem firmware that has been installed and will be installed into memory after the managed system is powered off and powered on.

Activated level

This is the level of server firmware or power subsystem firmware that is active and running in memory.

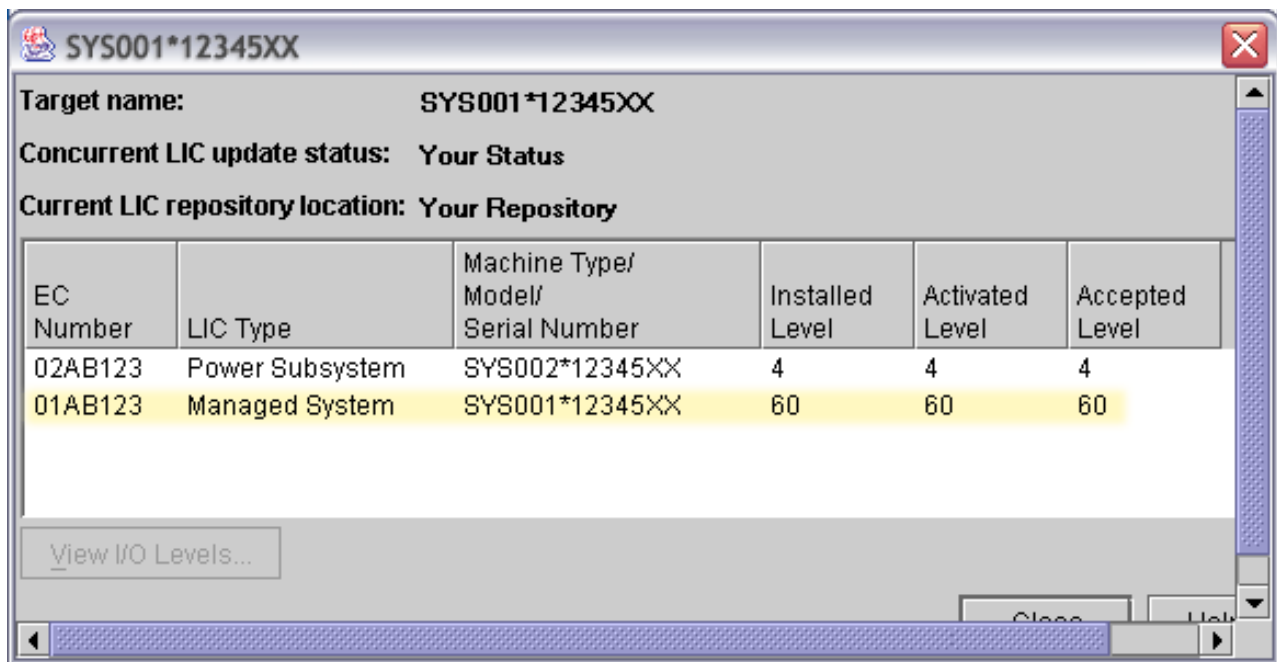
Accepted level

This is the backup level of server or power subsystem firmware. You can return to this level of server or power subsystem firmware if you decide to remove the installed level.

The existing levels of server firmware or power subsystem firmware are displayed 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.

Figure 48. A panel from the HMC interface that highlights the levels of server firmware on the target system.



For instructions on how to view the levels of server firmware and power subsystem firmware, see [Viewing existing firmware levels](#).

Related tasks

“Viewing existing firmware levels” on page 186

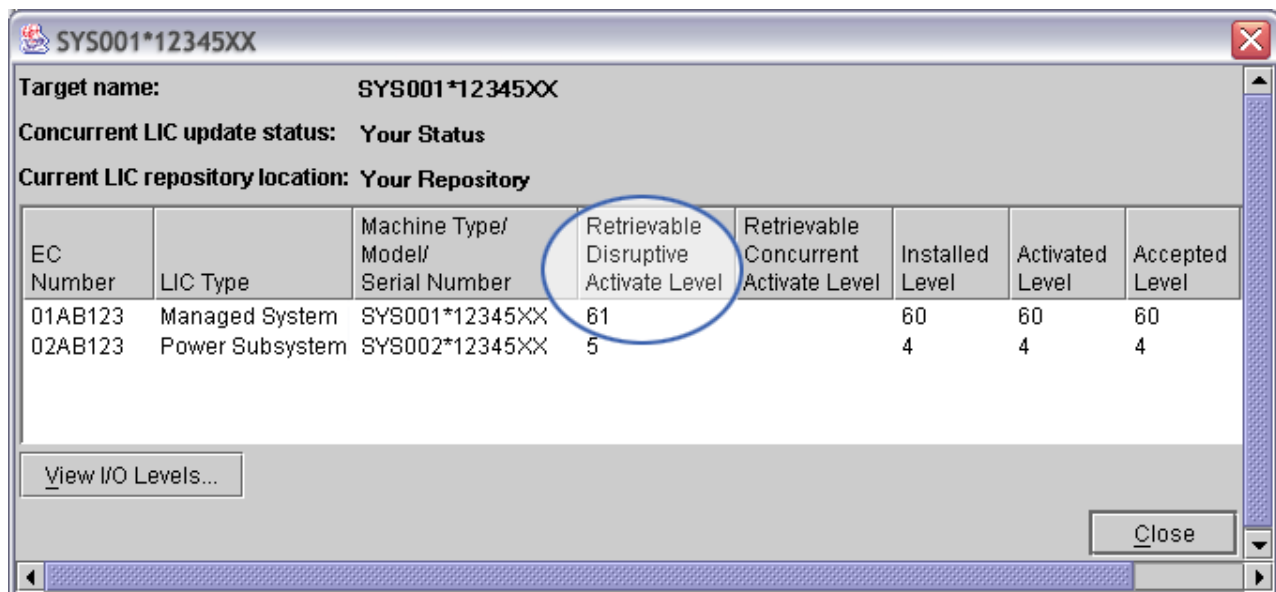
Find out how to view the level of firmware that currently runs on your server.

Available levels of server firmware and power subsystem firmware: When service and support releases server firmware and power subsystem firmware updates, you can view the available levels that can be downloaded and installed from each repository to your server.

The following figure highlights the retrievable level of server firmware and power subsystem firmware. See the detailed descriptions that follow the figure.

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

Figure 49. This diagram shows a panel from the HMC interface that highlights the retrievable disruptive level of server firmware and power subsystem firmware.



- **Retrievable disruptive activate level** – This is the highest level of server or power subsystem firmware available at the selected repository. Activation of this level is a disruptive process. Therefore, you will be instructed to shut down all of the applications and logical partitions before initiating the installation. 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 or power subsystem firmware available at the selected repository that can be retrieved, installed, and activated concurrently. Activation of this level 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 update.

For instructions on how to view the available levels of server firmware and power subsystem firmware, see Viewing available firmware (Licensed Internal Code) levels.

Related tasks

“Viewing available firmware levels” on page 190

Find out how to view the levels of firmware that are available for you to download as fixes.

Understanding concurrent firmware maintenance using the HMC

Learn about performing concurrent firmware maintenance using the HMC.

Concurrent firmware maintenance allow you to apply firmware updates on a running system without shutting down and restarting logical partitions, servers, or stopping applications. However, not every firmware update is concurrent.

To perform concurrent activation requires an HMC, and updates through the operating system will still be disruptive.

Currently, server firmware updates can be concurrent or disruptive. Power subsystem updates are concurrent with respect to server operations. HMC machine code is updated in a separate update. The HMC machine code updates are concurrent with respect to the managed systems.

Only updates within a release can be (but are not guaranteed to be) concurrent.

- The release level is indicated by the three numbers after “SF” in the level name. For example, in the firmware level SF230_126, the release level is 230.
- Installing a newer release is always disruptive. For example, if the server has SF225 installed, and you install SF230, the installation will be disruptive (the managed system will be shut down and restarted).

To update firmware, you will be performing the following steps:

1. Apply the firmware (update what is in flash).
2. Activate the firmware (cause the new firmware to be running on the system).

Not all updates can be activated concurrently. The types of activations include:

- **Concurrent:** Apply and activate with partitions running.
- **Deferred:** Concurrent activation but contains updates that affect the initial program load (IPL) path, which are not activated until the next time you shut down and restart the server.

Note: The portions of the update that can be activated concurrently are activated as described earlier.

- **Disruptive:** Platform shutdown and restart is required; that is, none of the update contents are activated until the next time you shut down and restart the server.

For more information on concurrent updates, refer to Performing Licensed Internal Code Maintenance module in IBM Resource Link™.

Related information

 [POWER5 Code Matrix Web site](#)

Applying firmware to multiple managed systems using an HMC

Learn more about applying firmware to multiple managed systems using an HMC.

When using the HMC to perform firmware updates and upgrades, you can select multiple managed systems to be updated simultaneously from the Target Object Selection window. If the DVD repository is used during an *upgrade*, then the upgrade will be performed sequentially. For details, refer to “DVD repository limitations.”

Also, if you are updating or upgrading a 575 system, review the following considerations in “Considerations for updating firmware on a 575 system.”

DVD repository limitations: The DVD drive will be locked while you are using the DVD as a repository. If you are updating within the same release, this will be performed simultaneously. When you are *upgrading* to a new release (for example: upgrading from the 230 release to the 235 release), this will be done sequentially. That is, the DVD drive will be locked for a longer period of time. Therefore, another repository might be preferred.

Note: Do not upgrade multiple managed systems to a new release from a DVD repository if you want the managed systems to be upgraded simultaneously.

Considerations for updating firmware on a 575 system: Updates of multiple managed systems in a 575 system can cause the potential for a lock conflict on the power frame. To obtain the most parallel processing during firmware updates on a 575 system, perform the following update sequence:

1. Select one managed system target in each power frame, and update the firmware. These targets will be updated in parallel.
2. Select all remaining managed system targets, and update the firmware. These targets will be updated in parallel.

Note: You can also update multiple managed systems from the HMC command line using the `updlc` command.

Temporary and permanent side of the service processor when using an HMC

Learn about the two sides of the service processor that store the server firmware.

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: By default, the server firmware is installed on the temporary side only after the existing contents of the temporary side are permanently installed on the permanent side. (This process is performed automatically when you install a server firmware update.) If you want to preserve the contents of the permanent side, select **Install and Activate** from the Advanced Features on the HMC interface, and indicate that you do *not* want to automatically accept the firmware level.

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. For more details, see *Installing a firmware fix permanently*.

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. For details, see *Removing the current firmware level*. 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*.

Related tasks

"Installing a firmware update permanently" on page 170

Find out how to permanently install a firmware update.

"Removing the current firmware level" on page 195

Find out how to remove the current level of firmware so you can return to a previous level of server firmware or power subsystem firmware.

Related information

 Specifying the connection type from the HMC

Obtaining updates

Learn how to apply updates, including for the HMC machine code, server firmware, power subsystem, I/O adapter and device, and operating system.

How you apply updates will depend on the type of update that you are applying, whether you have an Internet connection from your HMC or server, and the operating system that you are using.

Obtaining HMC machine code updates and upgrades

Learn how to obtain HMC machine code updates and upgrades.

Updates are periodically released for the HMC to add new functionality and to improve existing features.

Obtaining machine code updates for the HMC with an Internet connection:

Learn how to obtain machine code updates for the HMC when the HMC has an Internet connection.

To obtain machine code updates for the HMC, perform Steps 1 through 5.

Step 1. Ensure that you have an Internet connection:

To download updates from the service and support system or Web site to your HMC or server, you must have a connection to service and support either through a modem, direct or indirect Internet, or pass-through system.

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
 - a. In the navigation area, open **Service Applications**.
 - b. Select **Remote Support**.
 - c. Select **Customize Outbound Connectivity**.
 - d. Continue with step 4.
3. Perform the following steps:
 - a. In the Navigation area, click **Service Management**.
 - b. Select **Manage Outbound Connectivity**.
4. Select the tab for the type of outbound connectivity that you chose for your HMC (Local Modem, Internet VPN, or Pass-Through Systems). For more information about these settings, see Specifying the connection type from the HMC.

Note: If a connection to service and support does not exist, set up the service connection before proceeding with this procedure. For instructions on how to set up a connection to service and support, see Setting up your server to connect to service and support.

5. Click **Test**.
6. Verify that the test completes successfully. If the test is not successful, troubleshoot your connectivity and correct the problem before proceeding with this procedure. Alternatively, you can obtain the update on CD.
7. Continue with "Step 2. View the existing HMC machine code level."

Related concepts

"Setting up your server to connect to service and support" on page 31
Learn about setting up your server to connect to service and support.


Related tasks

"Specifying the connection type from the HMC" on page 107
Learn how to specify the connection type from the HMC.

Step 2. View the existing HMC machine code level:

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using a an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
 - a. In the navigation area, open **Licensed Internal Code Maintenance**.
 - b. Select **HMC Code Update**.
 - c. In the contents area, view and record the version and release of your HMC machine code in the Status area.
 - d. Continue with step 4.
3. Perform the following steps:
 - a. In the Navigation area, click **Updates**.
 - b. In the Work area, view and record the information that appears under the HMC Code Level heading, including: the HMC version, release, maintenance level, build level, and base versions.
4. Continue with "Step 3. View the available HMC machine code levels" on page 123.

Step 3. View the available HMC machine code levels:

1. From a computer or server with an Internet connection, go to the Fix Central Web site at <http://www.ibm.com/eserver/support/fixes/> .
2. Select the appropriate family in the Product family list.
3. Select **Hardware Management Console** in the Product or fix type list.
4. Click **Continue**. The Hardware Management Console site is displayed.
5. Scroll down to your HMC Version level to view available HMC levels.

Note: If you prefer, you can contact service and support.

6. Continue with "Step 4. Apply the HMC machine code update."

Step 4. Apply the HMC machine code update:

1. Before you install updates to the HMC machine code, back up critical console information on your HMC. For instructions, see Backing up critical HMC data. Then continue with the next step.
2. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier , continue with step 3.
 - If you are using a HMC with Version 7 or later, continue with step 4.
3. Perform the following steps:
 - a. In the navigation area, expand the **Licensed Internal Code Maintenance** folder.
 - b. Select **HMC Code Update**.
 - c. Continue with step 5.
4. Perform the following steps:
 - a. In the Navigation area, click **Updates**.
 - b. Click **Update HMC**. The Install Corrective Service window opens.
5. Select **Install Corrective Service**. *Corrective service* refers to the HMC machine code update.
6. On the Install Corrective Service window, select **Download the corrective service file from a remote system, and then apply downloaded service file**, and enter the following information:
 - **Remote site:** ftp.software.ibm.com
 - **Patch file:** Enter the following FTP directory and ZIP file name: /software/server/hmc/fixes/*filename.zip*

Note:

- The name of the patch file changes with each new update.
To find the name of the patch file, go to the Hardware Management Console Web site at <http://www14.software.ibm.com/webapp/set2/sas/f/hmc/home.html>.
- You might need more than one zip file for an update.

- **User ID:** anonymous
- **Password:** Your e-mail address

7. Click **OK**.
8. Follow the instructions to install the update.
9. Shut down and restart the HMC for the update to take effect.

Related information

Backing up critical HMC data

Step 5. Verify that the HMC machine code update installed successfully:

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2 on page 124.

- If you are using an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
 - a. In the navigation area, open **Licensed Internal Code Maintenance**.
 - b. Select **HMC Code Update**.
 - c. In the contents area, look for the version and release of your HMC machine code in the Status area.
 - d. Verify that the version and release match the fix that you installed.
 - e. Continue with step 4.
 3. Perform the following steps:
 - a. In the Navigation area, click **Updates**.
 - b. In the Work area, the HMC version, release, maintenance level, build level, and base versions are displayed under the HMC Code Level heading.
 - c. Verify that the version and release match the update that you installed.
 4. If the level of code displayed is not the level that you installed, perform the following steps:
 - a. Check the network connection on the HMC.
 - b. Retry the firmware update using a different repository.
 - c. If the problem persists, contact your next level of support.

Obtaining machine code updates for the HMC using CD or an FTP server:


Learn how to obtain machine code updates for the HMC using CD or an FTP server.

To obtain HMC machine code updates, perform Steps 1 through 5.

Step 1. View the existing HMC machine code level:

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
 - a. In the navigation area, open **Licensed Internal Code Maintenance**.
 - b. Select **HMC Code Update**.
 - c. In the contents area, view and record the version and release of your HMC machine code in the Status area.
 - d. Continue with step 4.
3. Perform the following steps:
 - a. In the Navigation area, click **Updates**.
 - b. In the Work area, view and record the information that appears under the HMC Code Level heading, including: the HMC version, release, maintenance level, build level, and base versions.
4. Continue with "Step 2. View the available HMC machine code levels."

Step 2. View the available HMC machine code levels:


1. From a computer or server with an Internet connection, go to the Fix Central Web site at <http://www.ibm.com/eserver/support/fixes/> .
2. Select the appropriate family in the Product family list.
3. Select **Hardware Management Console** in the Product or fix type list.
4. Click **Continue**. The Hardware Management Console site is displayed.
5. Scroll down to your HMC Version level to view available HMC levels.

Note: If you prefer, you can contact service and support.

6. Continue with “Step 3. Obtain the HMC machine code update.”

Step 3. Obtain the HMC machine code update:

You can order the HMC machine code update through the Fix Central Web site, contact service and support, or download it to an FTP server.

1. From a computer or server with an Internet connection, go to the Fix Central Web site at <http://www.ibm.com/eserver/support/fixes/> .
2. Select the appropriate family in the Product family list.
3. Select **Hardware Management Console** in the Product or fix type list.
4. Click **Continue**. The Hardware Management Console site is displayed.
5. Under Supported HMC products, select the latest HMC level that supports POWER5 processors.
6. Scroll down to the File name(s) / Package area and locate the update you want to order.
7. In the Order CD column, select **Go**.
8. Click **Continue** to sign in with your IBM ID.
9. Follow the on-screen prompts to submit your order.

Note: If you do not have access to the Internet, contact service and support to order the update on CD.

10. Continue with “Step 4. Apply the HMC machine code update.”

Step 4. Apply the HMC machine code update:

1. Before you install updates to the HMC machine code, back up critical console information on your HMC. For instructions, see Backing up critical HMC data. Then continue with the next step.
2. If you obtained or created the update on CD, insert it into the CD drive on the HMC.
3. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 4.
 - If you are using an HMC with Version 7 or later, continue with step 5.
4. Perform the following steps:
 - a. In the navigation area, expand the **Licensed Internal Code Maintenance** folder.
 - b. Select **HMC Code Update**.
 - c. Continue with step 6.
5. Perform the following steps:
 - a. In the Navigation area, click **Updates**.
 - b. Click **Update HMC**. The Install Corrective Service window opens.
6. Select **Install Corrective Service**. *Corrective service* refers to the HMC machine code update.
7. On the Install Corrective Service window, choose from the following options:
 - If you want to download the update from an FTP server to your HMC, continue with step 8.
 - If you want to get the update from a CD, select **Apply corrective service from removable media** and continue with step 9 on page 126.
8. If you previously downloaded the update to an FTP server, select **Download the corrective service file from a remote system, and then apply downloaded service file**, and 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 update.
 - **Patch file:** The name of the patch file (zip file) that you downloaded to the FTP server.
 - **User ID:** Your user ID for the FTP server.

- **Password:** Your password for the FTP server.
9. Click **OK**.
 10. Follow the instructions to install the update.
 11. Shut down and restart the HMC for the update to take effect.
 12. Continue with “Step 5. Verify that the HMC machine code update installed successfully.”

Related information

Backing up critical HMC data

Step 5. Verify that the HMC machine code update installed successfully:

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
 - a. In the navigation area, open **Licensed Internal Code Maintenance**.
 - b. Select **HMC Code Update**.
 - c. In the contents area, look for the version and release of your HMC machine code in the Status area.
 - d. Verify that the version and release match the fix that you installed.
 - e. Continue with step 4.
3. Perform the following steps:
 - a. In the Navigation area, click **Updates**.
 - b. In the Work area, the HMC version, release, maintenance level, build level, and base versions are displayed under the HMC Code Level heading.
 - c. Verify that the version and release match the update that you installed.
4. If the level of code displayed is not the level that you installed, perform the following steps:
 - a. Retry the machine code update. If you created a CD or DVD for this procedure, use a new media.
 - b. If the problem persists, contact your next level of support.

Updating the code on multiple HMCs using the remote command line:

Learn how to use the HMC remote command line to update the code on more than one HMC at a time.

To remotely install interim updates, service packs, and cumulative maintenance releases on the HMC, use the `updhmc` command. The following example illustrates a scenario where an HMC code update is performed on multiple HMC machines from a remote system.

In this scenario, System A is a Linux system installed with OpenSSH. Assume that public key files have been previously deployed to all the HMCs, and these key files were generated with an empty passphrase.

```
for i in 1 2 3 4 5 6 7
do
  scp hmc_update.zip hscroot@hmc$i:/home/hscroot
done
for i in 1 2 3 4 5 6 7
do
  ssh hscroot@hmc$i "updhmc -t 1 -f /home/hscroot/hmc_update.zip -c -r"
done
```


The first <for> loop in the preceding code example copies an interim update called hmc_update.zip to 7 HMCs, with host name hmc1, hmc2, ..., hmc7. The second <for> loop runs the updhmc command on each of the 7 HMCs. When the updhmc command completes, it removes the file and shuts down and restarts the HMC.

Upgrading the machine code on an HMC:

Learn how to upgrade the machine code on an HMC from one release to the next while maintaining your HMC configuration data.


Perform Steps 1 through 9 to upgrade machine code on an HMC.

Notes:

- If you are upgrading from HMC with Version 6 to HMC Version 7, refer to “Upgrading the machine code on an HMC from Version 6 to Version 7” on page 132.
- You cannot use this procedure to upgrade from a POWER4™ HMC to a POWER5 HMC. You must do a full installation.

Step 1. Obtain the upgrade:

You can order the HMC machine code upgrade through the Fix Central Web site, by contacting service and support, or by downloading it to an FTP server.

1. From a computer or server with an Internet connection, go to the Fix Central Web site at <http://www.ibm.com/eserver/support/fixes/> .
2. Select the appropriate family in the Product family list.
3. Select **Hardware Management Console** in the Product or fix type list.
4. Click **Continue**. The Hardware Management Console site is displayed.
5. Navigate to the HMC version you want.
6. Locate the Recovery CD download and ordering section.

Note: If you do not have access to the Internet, contact service and support to order the upgrade on DVD.

7. Follow the on-screen prompts to submit your order.
8. After you have the upgrade, continue with “Step 2. View the existing HMC machine code level.”

Step 2. View the existing HMC machine code level:

To determine the existing level of machine code on an HMC, follow these steps:

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
 - a. In the navigation area, open **Licensed Internal Code Maintenance**.
 - b. Select **HMC Code Update**.
 - c. In the contents area, view and record the version and release of your HMC machine code in the Status area.
 - d. Continue with step 5 on page 128.
3. In the Navigation area, click **Updates**.
4. In the Work area, view and record the information that appears under the HMC Code Level heading, including: the HMC version, release, maintenance level, build level, and base versions.

5. Continue with "Step 3. Back up the managed system's profile data."

Step 3. Back up the managed system's profile data:

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using a an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
 - a. In the navigation area, select **Server and Partition**.
 - b. In the contents area, open **Server Management**. A task list displays.
 - c. Right-click the managed system and select **Profile data** → **Backup**.
 - d. Continue with step 4.
3. Perform the following steps:
 - a. In the Navigation area, select **Systems Management**.
 - b. Select **Servers**.
 - c. Select the server and ensure the state is *Operating* or *Standby*.
 - d. Under Tasks, select **Configuration** → **Manage Partition Data** → **Backup**.
4. Type a backup file name and record this information.
5. Click **OK**.
6. Repeat these steps for each managed system.
7. Continue with "Step 4. Back up critical console information or HMC Data."

Step 4. Back up critical console information or HMC Data:

Back up critical console information or HMC Data before installing a new version of HMC software so that previous levels can be restored in the event of a problem while upgrading the software. Do not use this critical console data after a successful upgrade to a new version of the HMC software.

Note: If you choose to back up to removable media (that is, diskette or DVD), you will need to have a diskette or DVD available.

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 3.
2. If you plan to back up to diskette or DVD-RAM, perform the following steps:
 - a. Insert the media into the drive.
 - b. Select **Format Removable Media**.
 - c. Select **Format DVD-RAM** or **Format diskette**.
 - d. Click **OK**.
 - e. Select **Back up Critical Console Data**.
 - f. Continue with step 4 on page 129.
3. If you plan to back up to USB flash drive or DVD-RAM, perform the following steps:
 - a. Insert the media into the drive.
 - b. In the Navigation Pane, select **Service Management**
 - c. Select **Format Media**.
 - d. Select **Format DVD-RAM** or **Format high speed memory key**.
 - e. Click **OK**.
 - f. In the Navigation area, select **HMC Management**.
 - g. Select **Back up HMC Data**. The back up critical console data window appears.

4. Select an archive option. You can back up to a DVD in the HMC, a remote system mounted to the HMC file system (for example, NFS), or send the back up to a remote site using File Transfer Protocol (FTP).
 - To back up to DVD, choose **Back up to DVD on local system** and follow the instructions.
 - To back up to a mounted remote system, choose **Backup to mounted remote system** and follow the instructions.
 - To back up to a remote FTP site, choose **Send backup critical data to remote site** and follow the instructions.
5. Continue with “Step 5. Record the current HMC configuration information.”

Step 5. Record the current HMC configuration information:

Before you upgrade to a new version of HMC software, as a precautionary measure, record HMC configuration information.

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
 - a. In the navigation area, open **HMC Management**.
 - b. Select **HMC Configuration**.
 - c. Continue with step 4.
3. In the Navigation area, select **HMC Management**.
4. In the tasks list, select **Schedule Operations**. The Scheduled Operations window displays with a list of all managed systems.
5. Select the HMC you plan to upgrade and click **OK**. All scheduled operations for the HMC are displayed.
6. Select **Sort → By Object**.
7. Select each object and record the following details:
 - Object Name
 - Schedule date
 - Operation Time (displayed in 24-hour format)
 - Repetitive (if *Yes*, perform the following steps):
 - a. Select **View → Schedule Details**.
 - b. Record the interval information.
 - c. Close the scheduled operations window.
 - d. Repeat for each scheduled operation.
8. Close the Customize Scheduled Operations window.
9. Continue with “Step 6. Record remote command status.”

Step 6. Record remote command status:

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 3 on page 130.
2. Perform the following steps:
 - a. In the navigation area, select **HMC Management**.
 - b. Select **HMC Configuration**.
 - c. In the tasks list, click **Enable/Disable Remote Command Execution**.
 - d. Continue with step 5 on page 130.

3. In the navigation area, select **HMC Management**.
4. In the tasks list, click **Remote Command Execution**.
5. Record whether the **Enable remote command execution using the ssh facility** check box is selected.
6. Click **Cancel**.
7. Continue with "Step 7. Save upgrade data."

Step 7. Save upgrade data:

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

Note: Only one level of backup data is allowed. Each time you save upgrade data, the previous level is overwritten.

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 3.
 2. Perform the following steps:
 - a. In the navigation area, open the **Licensed Internal Code** folder.
 - b. Select **HMC Code Update**.
 - c. Select **Save Upgrade Data**.
 - d. Select **Hard Drive** and click **Continue**.
 - e. Click **Continue** to start the task.
 - f. Continue with step 4.
 3. Perform the following steps:
 - a. In the Navigation area, select **HMC Management**.
 - b. In the contents area under Operations, select **Save Upgrade Data**.
 - c. Select **Hard Drive** and click **Next**.
 - d. Click **Finish**.
 4. Wait for the task to complete. If the Save Upgrade Data task fails, contact your next level of support before proceeding.
- Note:** If the save upgrade data task fails, do not continue the upgrade process.
5. Click **OK**.
 6. Click **Close**.
 7. Continue with "Step 8. Upgrade the HMC software."

Step 8. Upgrade the HMC software:

To upgrade the HMC software, you restart the system with the DVD-RAM in the DVD-RAM drive.

1. Insert the HMC Product Installation DVD-RAM into the DVD-RAM drive.
2. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 3.
 - If you are using an HMC with Version 7 or later, continue with step 4 on page 131.
3. Perform the following steps:
 - a. From the HMC menu bar, select **Console** → **Exit**.
 - b. Click **Exit now**.

- c. From the logout list, select **Reboot Console** and click **OK**. The HMC restarts and system information scrolls on the window.
- d. Continue with step 5.
4. Perform the following steps:
 - a. In the Navigation bar, select **HMC Management**.
 - b. In the contents area, select **Shutdown or Restart HMC**.
 - c. Ensure **Restart the HMC** is selected.
 - d. Click **OK**. The HMC restarts and system information scrolls on the window.
5. Select **Upgrade** and click **Next**.
6. When the warning is displayed, choose from the following options:
 - If you have saved upgrade data during the previous task, continue with the next step.
 - If you did not save upgrade data previously in this procedure, you must save the upgrade data now before you continue.
7. Select **Upgrade from media** and click **Next**.
8. Confirm the settings and click **Finish**.
9. Follow the on-screen prompts.

Note:

- If the screen goes blank, press the space bar to view the information.
 - The first DVD can take approximately 20 minutes to install.
10. When prompted, remove the first media and then insert the second media into the DVD-RAM drive.
 11. Select **1. Install additional software from media** and press Enter. Press any key to confirm the installation. The HMC will display status messages as it installs the packages.
 12. When the second media installation is complete, remove the media from the drive and close the drawer.
 13. Select **Option 2 Finish the installation** and press Enter. The HMC will complete the booting process.
 14. Accept the License Agreement for Machine Code twice.
 15. At the login prompt, log in using your user ID and password. The HMC code installation is complete.
 16. Continue with "Step 9. Verify that the HMC machine code upgrade installed successfully."

Step 9. Verify that the HMC machine code upgrade installed successfully:

To verify that the HMC upgrade installed successfully, perform these steps:

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
 - a. In the navigation area, open **Licensed Internal Code Maintenance**.
 - b. Select **HMC Code Update**.
 - c. In the contents area, look for the version and release of your HMC machine code in the Status area.
 - d. Verify that the version and release match the fix that you installed.
 - e. Continue with step 4 on page 132.
3. Perform the following steps:
 - a. In the Navigation area, click **Updates**.
 - b. In the Work area, the HMC version, release, maintenance level, build level, and base versions are displayed under the HMC Code Level heading.

- c. Verify that the version and release match the update that you installed.
4. If the level of code displayed is not the level that you installed, perform the following steps:
 - a. Retry the upgrade task using a new DVD.
 - b. If the problem persists, contact your next level of support.

Upgrading the machine code on an HMC from Version 6 to Version 7:


Learn how to upgrade the machine code on an HMC from Version 6 to Version 7 while maintaining your HMC configuration data.

Perform Steps 1 through 9 to upgrade machine code on an HMC from Version 6 to Version 7.

Important: You must be at a minimum of HMC machine code Version 6 Release 1.2 to upgrade to Version 7 Release 3.1.0.

Step 1. Obtain the upgrade:

You can order the HMC machine code upgrade through the Fix Central Web site, by contacting service and support, or by downloading it to an FTP server.

1. From a computer or server with an Internet connection, go to the Fix Central Web site at <http://www.ibm.com/eserver/support/fixes/> .
2. Select the appropriate family in the Product family list.
3. Select **Hardware Management Console** in the Product or fix type list.
4. Click **Continue**. The Hardware Management Console site is displayed.
5. Navigate to the HMC version you want.
6. Locate the Recovery CD download and ordering section.

Note: If you do not have access to the Internet, contact service and support to order the upgrade on DVD.

7. Follow the on-screen prompts to submit your order.
8. After you have the upgrade, continue with "Step 2. View the existing HMC machine code level."

Step 2. View the existing HMC machine code level:

To determine the existing level of machine code on an HMC, follow these steps:

1. In the navigation area, expand the **Licensed Internal Code Maintenance** folder.
2. Select **HMC Code Update**.
3. In the Status area, look for the version and release of your HMC machine code.
4. Record the current version and release.

Important: You must be at a minimum of Version 6 Release 1.2 to upgrade to HMC machine code Version 7 Release 3.1.0.

5. Continue with "Step 3. Back up the managed system's profile data."

Step 3. Back up the managed system's profile data:

1. In the navigation area, select **Server and Partition**.
2. In the contents area, open **Server Management**. A task list displays.
3. Right-click the managed system and select **Profile data** → **Backup**.
4. Type a backup file name and record this information.
5. Click **OK**.

6. Repeat steps 3 on page 132 through 5 on page 132 for each managed system.
7. Continue with “Step 4. Back up critical console information.”

Step 4. Back up critical console information:

Back up critical console information before installing a new version of HMC software so that previous levels can be restored in the event of a problem while upgrading the software. Do not use this critical console data after a successful upgrade to a new version of the HMC software.

Note: If you choose to back up the console data to removable media (that is, diskette or DVD), you will need to have a diskette or DVD available.

1. Choose from the following options:
 - If you do *not* plan to back up to diskette or DVD-RAM, continue with the next step.
 - If you plan to back up to diskette or DVD-RAM, perform the following steps:
 - a. Insert the media into the drive.
 - b. Select **Format Removable Media**.
 - c. Select **Format DVD-RAM** or **Format diskette**.
 - d. Click **OK**.
 - e. Continue with the next step.
2. Select **Back up Critical Console Data**.
3. Select an archive option. You can back up to a DVD in the HMC, a remote system mounted to the HMC file system (for example, NFS), or send the back up to a remote site using File Transfer Protocol (FTP).
 - To back up to DVD, choose **Back up to DVD on local system** and follow the instructions.
 - To back up to a mounted remote system, choose **Backup to mounted remote system** and follow the instructions.
 - To back up to a remote FTP site, choose **Send backup critical data to remote site** and follow the instructions.
4. Continue with “Step 5. Record the current HMC configuration information.”

Step 5. Record the current HMC configuration information:

Before you upgrade to a new version of HMC software, as a precautionary measure, record HMC configuration information.

To record HMC configuration information, follow these steps:

1. In the navigation area, open **HMC Management**.
2. Select **HMC Configuration**.
3. In the tasks list, select **Schedule Operations**. The Scheduled Operations window displays with a list of all managed systems.
4. Select the HMC you plan to upgrade and click **OK**. All scheduled operations for the HMC are displayed.
5. Select **Sort → By Object**.
6. Select each object and record the following details:
 - Object Name
 - Schedule date
 - Operation Time (displayed in 24-hour format)
 - Repetitive (if Yes, perform the following steps:
 - a. Select **View → Schedule Details**.

- b. Record the interval information.
 - c. Close the scheduled operations window.
 - d. Repeat for each scheduled operation.
7. Close the Customize Scheduled Operations window.
 8. Continue with "Step 6. Record remote command status."

Step 6. Record remote command status:

1. In the navigation area, select **HMC Management**.
2. Select **HMC Configuration**.
3. In the tasks list, click **Enable/Disable Remote Command Execution**.
4. Record whether the **Enable remote command execution using the ssh facility** check box is selected.
5. Click **Cancel**.
6. Continue with "Step 7. Save upgrade data."

Step 7. Save upgrade data:

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

Note: Only one level of backup data is allowed. Each time you save upgrade data, the previous level is overwritten.

1. In the navigation area, open the **Licensed Internal Code** folder.
2. Select **HMC Code Update**.
3. Select **Save Upgrade Data**.
4. Select **Hard Drive** and click **Continue**.
5. Click **Continue** to start the task.
6. Wait for the task to complete. If the Save Upgrade Data task fails, contact your next level of support before proceeding.

Note: If the save upgrade data task fails, do not continue the upgrade process.

7. Click **OK**.
8. Click **Close**.
9. Continue with "Step 8. Upgrade the HMC software from Version 6 to Version 7."

Step 8. Upgrade the HMC software from Version 6 to Version 7:

To upgrade the HMC software, you restart the system with the DVD-RAM in the DVD-RAM drive.

1. Insert the HMC Product Installation DVD-RAM into the DVD-RAM drive.
2. Perform the following steps:
 - a. From the HMC menu bar, select **Console** → **Exit**.
 - b. Click **Exit now**.
 - c. From the logout list, select **Reboot Console** and click **OK**. The HMC restarts and system information scrolls on the window.
3. Select **Upgrade** and click **Next**.
4. When the warning is displayed, choose from the following options:
 - If you have saved upgrade data during the previous task, continue with the next step.
 - If you did not save upgrade data previously in this procedure, you must save the upgrade data now before you continue.

5. Select **Upgrade from media** and click **Next**.
6. Confirm the settings and click **Finish**.
7. Follow the on-screen prompts.

Note:

- If the screen goes blank, press the space bar to view the information.
 - The first DVD can take approximately 20 minutes to install.
8. When prompted, remove the first media and then insert the second media into the DVD-RAM drive.
 9. Select **1. Install additional software from media** and press Enter. Press any key to confirm the installation. The HMC will display status messages as it installs the packages.
 10. When the second media installation is complete, remove the media from the drive and close the drawer.
 11. Select **Option 2 Finish the installation** and press Enter. The HMC will complete the booting process.
 12. Accept the License Agreement for Machine Code twice.
 13. At the login prompt, log in using your user ID and password. The HMC code installation is complete.
 14. Continue with "Step 9. Verify that the HMC machine code upgrade installed successfully."

Step 9. Verify that the HMC machine code upgrade installed successfully:

1. In the Navigation area, click **Updates**.
2. In the Work area, the HMC version, release, maintenance level, build level, and base versions are displayed under the HMC Code Level heading.
3. Verify that the version and release match the update that you installed.
4. If the level of code displayed is not the level that you installed, perform the following steps:
 - a. Retry the update using a different DVD.
 - b. If the problem persists, contact your next level of support.

Obtaining firmware updates

Learn how to obtain firmware updates.

Server firmware enables hardware, such as the service processor. When you install a server firmware update it is installed on the temporary side of the service processor.

The power subsystem firmware is the part of the Licensed Internal Code that enables the power subsystem hardware in the model 575 and 59x servers. You must use an HMC to update or upgrade power subsystem firmware.

How you apply updates will depend on the type of update that you are applying, and whether you have an Internet connection from your HMC or server.

Obtaining server firmware updates for a 7037-A50 or 7047-185 system:

Learn how to update or upgrade server firmware for a 7037-A50 or 7047-185 system.

Installing server firmware updates through the operating system is a disruptive process.

Perform Steps 1 through 6 to get server firmware updates through AIX or Linux when you have a 7037-A50 or 7047-185 system.

Note: If you are unable to start your AIX or Linux operating system or server, refer to Obtaining server firmware updates through AIX or Linux when you are unable to start the operating system or server.

Related tasks

“Obtaining server firmware updates through AIX or Linux when you are unable to start the operating system or server” on page 202

Learn how to apply server firmware updates through AIX or Linux when you are unable to start the operating system or server.

Step 1. View existing firmware levels for AIX or Linux:

1. Choose from the following options:

- To use the AIX command prompt (you must have AIX diagnostics installed on your server to perform this task), continue with step 2.
- To use the Linux command prompt, continue with step 4.

2. At an AIX command prompt, enter the following command:

```
lsmcode
```

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

```
The current permanent system firmware image is AT061_055.  
The current temporary system firmware image is AT061_058.  
The system is currently booted from the temporary image.
```

Note: When the lsmcode command is run on a 7037-A50 or 7047-185 system, the temporary or permanent side of the flash might report `_UNKNOWN_` for the firmware level. This occurs because there is only one level of base motherboard controller firmware. The level is `_UNKNOWN_` when it is not included with the system firmware.

When you install new firmware, it is installed onto the temporary side by default. This new firmware level includes a new level of base motherboard controller code, and will cause `_UNKNOWN_` to be reported for the permanent side. This is not a problem; it indicates that the firmware levels in the flash are not a combination that is included from the factory.

To update the firmware so that `_UNKNOWN_` is not reported, perform the following steps:

- a. Perform a commit operation using the appropriate operating system command.
- b. After the commit operation is complete, restart the system.
- c. When the system has restarted and the operating system is running, rerun the lsmcode command. Both the T and P should report a level (such as AT206_061) instead of `_UNKNOWN_`.

3. Continue with “Step 2. View or download the firmware update” on page 137.

4. To view existing levels of server firmware for Linux, you must have the following service tools installed on 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.

Note: If you do not have the service tools on your server, refer to “Obtaining service and productivity tools for Linux” on page 207.

5. After the service tools are installed to the server running Linux, enter the following at a Linux command prompt:

```
lsmcode
```

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

```
Version of system firmware is: AT061_058(t) AT061_055(p) AT061_058(t)
```

Note: When the `lsmcode` command is run on a 7037-A50 or 7047-185 system, the temporary or permanent side of the flash might report `_UNKNOWN_` for the firmware level. This occurs because there is only one level of base motherboard controller firmware. The level is `_UNKNOWN_` when it is not included with the system firmware.

When you install new firmware, it is installed onto the temporary side by default. This new firmware level includes a new level of base motherboard controller code, and will cause `_UNKNOWN_` to be reported for the permanent side. This is not a problem; it indicates that the firmware levels in the flash are not a combination that is included from the factory.

To update the firmware so that `_UNKNOWN_` is not reported, perform the following steps:

- a. Perform a commit operation using the appropriate operating system command.
- b. After the commit operation is complete, restart the system.
- c. When the system has restarted and the operating system is running, rerun the `lsmcode` command. Both the T and P should report a level (such as `AT206_061`) instead of `_UNKNOWN_`.

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

AT061_058 (t)

The temporary level.

AT061_055 (p)

The permanent level.

AT061_058 (t)

The level on which the server is currently running.

6. Continue with "Step 2. View or download the firmware update."


Related tasks

"Obtaining service and productivity tools for Linux" on page 207

Find out about obtaining service and productivity tools for Linux.

Step 2. View or download the firmware update:

Follow this procedure to view or download the firmware update. You can download the update directly to your server, or you can download it to a computer with an Internet connection and create an update CD that you apply on the server. If necessary, contact service and support to order the update on CD.

1. From a computer or server with an Internet connection, go to the Fix Central Web site at <http://www.ibm.com/eserver/support/fixes/> .
2. Select the appropriate family in the Product family list.
3. Select **Hardware Management Console** in the Product or fix type list.
4. Click **Continue**. The Hardware Management Console site is displayed.
5. From the Microcode downloads Web site, perform the following steps:
 - a. Select your machine type and model from the drop-down list. An information window is displayed.
 - b. Click **Continue**. The available firmware levels are displayed.
 - c. Record the available firmware. If you want to download the update, continue with the next step.
6. Perform the following steps:
 - a. Select the **RPM** check box for the server firmware version you want.
 - b. Scroll to the bottom of the page and click **Continue**.
 - c. Click **Continue** again. The License Agreement is displayed.
 - d. Click **I agree to abide by its terms** and click **Continue**.
 - e. Follow the on-screen prompts.

7. Choose from the following options:

- If you downloaded the RPM file to your server, continue with “Step 3. View and unpack the RPM file that contains the server firmware.”
- If you want to create a CD containing the RPM file, follow the instructions for your CD program and then continue with “Step 3. View and unpack the RPM file that contains the server firmware.”

Step 3. View and unpack the RPM file that contains the server firmware:

If you downloaded or created a CD with the RPM file, you will need to view and unpack the RPM file that contains the server firmware.

1. Insert the CD that contains the RPM file into the media drive on your server.

2. To mount the CD, choose from the following options (you will need to have root user authority):

- If you are working on an AIX system, enter the following at an AIX command prompt:
`mount /dev/cd0 /mnt`
- If you are working on a Linux system, enter one of the following commands at a Linux command prompt:
`mount -t iso9660 /dev/cdrom /mnt`
or
`mount -t iso9660 /dev/dvdrom /mnt`

3. Choose from the following options:

- If the mount was *successful*, continue with step 5.
- If the mount was *unsuccessful*, continue with the next step.

4. If you received the message, `mount: 0506-324 Cannot mount /dev/cd0 on /mnt`, perform the steps below to mount the CD:

a. Enter the command:

```
/usr/sbin/mount -v 'cdrfs' -f'' -p'' -r'' /dev/cd0 /mnt
```

The quotation marks following the *f*, *p*, and *r* are two single quotation marks with no space between them.

Note: If you prefer to use the System Management Interface Tool (SMIT) to mount the CD, see “Using the System Management Interface Tool to mount the update CD for AIX” on page 206.

b. Continue with the next step.

5. To view the RPM file name, enter the following command at the AIX or Linux command prompt:

If the RPM file is on CD, type:

```
ls /mnt
```

If the RPM file is on the server, type:

```
ls /tmp/fwupdate
```

The name of the RPM file is displayed. For example, you might see output similar to the following:

```
AT2xx-yyy-2.rpm
```

6. To unpack the RPM file, enter one of the following commands at the AIX or Linux command prompt:

- If you want to unpack from a CD, enter:

```
rpm -Uvh --ignoreos /mnt/filename.rpm
```

- If you want to unpack from the server’s hard drive, enter:

```
rpm -Uvh --ignoreos /tmp/fwupdate/filename.rpm
```

where *filename* is the name of the RPM file that contains the server firmware. For example, `AT2xx-yyy-2.rpm`.

Note: When you unpack the RPM file, the server firmware update file is saved in the `/tmp/fwupdate` directory on the server's hard drive in the following format: `AT2xx-yyy-2.img`.

7. Continue with "Step 4. Apply server firmware updates through AIX or Linux to the temporary side of the service processor."

Related tasks

"Using the System Management Interface Tool to mount the update CD for AIX" on page 206

Use this procedure if you want to use SMIT to mount the update CD for AIX.

Step 4. Apply server firmware updates through AIX or Linux to the temporary side of the service processor:

1. Ensure you are starting the system from the temporary side of the service processor; the firmware installation will fail if the system has booted from the permanent side. To learn which side you are starting from, and how to change to the other side if necessary, refer to "Working with the temporary and permanent side of the service processor" on page 208.
2. To use the `update_flash` command (AIX or Linux) to install the server firmware, continue with step 3.

Note: If you have AIX installed, and prefer to use the AIX diagnostics to install the update, see Using the AIX diagnostics to install the server firmware update through AIX. If you plan to install the update from CD, you will need to obtain the *Microcode Updates Files & Discovery Tool* CD to use the AIX diagnostics.

3. You will need the server firmware update file name in the next step. To view the name, enter the following at an AIX or Linux command prompt:

```
ls /tmp/fwupdate
```

The name of the server firmware update file is displayed. For example, you might see output similar to the following:

```
AT2xx-yyy-2.img
```

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

4. To install the server firmware update, choose from the following options:

- If you are updating AIX, enter the following at an AIX command prompt:

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

where *fwlevel* is the specific server firmware update file name, such as `AT2xx-yyy-2.img`

- If you are updating Linux, enter the following at a Linux command prompt:

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

where *fwlevel* is the specific server firmware update file name, such as `AT2xx-yyy-2.img`

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

5. Continue with "Step 5. Verify that the update installed correctly."

Related tasks

"Working with the temporary and permanent side of the service processor" on page 208

Find out how to determine which side you are booting from, and how to switch to the other side if necessary.

"Using the AIX diagnostics to install the server firmware update through AIX" on page 204

Use this procedure if you want to use the AIX diagnostics to install the server firmware update through AIX to the temporary side of the service processor.

Step 5. Verify that the update installed correctly:

1. To use the AIX or Linux command prompt (the operating system must be running and the diagnostics must be available), continue with the next step.
2. Enter the following at a command prompt:

```
lsmcode
```

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

```
The current permanent system firmware image is AT061_055.  
The current temporary system firmware image is AT061_058.  
The system is currently booted from the temporary image.
```

Note: When the lsmcode command is run on a 7037-A50 or 7047-185 system, the temporary or permanent side of the flash might report `_UNKNOWN_` for the firmware level. This occurs because there is only one level of base motherboard controller firmware. The level is `_UNKNOWN_` when it is not included with the system firmware.

When you install new firmware, it is installed onto the temporary side by default. This new firmware level includes a new level of base motherboard controller code, and will cause `_UNKNOWN_` to be reported for the permanent side. This is not a problem; it indicates that the firmware levels in the flash are not a combination that is included from the factory.

To update the firmware so that `_UNKNOWN_` is not reported, perform the following steps:

- a. Perform a commit operation using the appropriate operating system command.
 - b. After the commit operation is complete, restart the system.
 - c. When the system has restarted and the operating system is running, rerun the lsmcode command. Both the T and P should report a level (such as AT206_061) instead of `_UNKNOWN_`.
3. Verify that the level of server firmware displayed is the level that you installed.
 4. If the level of server firmware displayed is not the level that you installed, perform the following steps:
 - a. Retry the update. If you created a CD or DVD for this procedure, use a new media.
 - b. If the problem persists, contact your next level of support.

Step 6. (Optional) Install the server firmware update 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 works correctly, you can permanently install the server firmware update.

Note: If you install the server firmware update 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 updates permanently, see “Installing a firmware update permanently” on page 170.

Related tasks

“Installing a firmware update permanently” on page 170
Find out how to permanently install a firmware update.

Obtaining updates for the Virtual I/O Server:

Learn about obtaining updates to the firmware on the Virtual I/O Server, and for the firmware on the devices that the Virtual I/O Server manages.

You can update the Virtual I/O Server's firmware and device microcode through the Integrated Virtualization Manager or by using the command line interface.

If you do not have an Internet connection from the system, you will need to obtain the update on CD.

You can use the information on the Virtual I/O Server update Web site to download and install the latest fix packs and updates on the management partition of the managed system. For more information about the methods that you can use to install these updates, see the Virtual I/O Server update Web site.

Related information

 [Virtual I/O Server update Web site](#)

Obtaining firmware updates through an HMC with an Internet connection:

Learn how to update or upgrade server firmware and power subsystem firmware (if you have a model 575 or 59x server) through an HMC when you have an Internet connection from the HMC or server.

Important: The HMC machine code needs to be equal to or greater than the server firmware level. Also, if an HMC manages multiple servers at different firmware release levels, the HMC machine code level must be equal to or higher than the system firmware level on the server that is at the latest release level. During this procedure you will find out how to ensure your HMC machine code and server firmware is compatible.

You *must* install HMC updates before you install server firmware or power subsystem firmware updates so that the HMC can handle any updates or new function that you apply to the server. After you install HMC updates, either install the power subsystem firmware and server firmware updates together, or install the power subsystem firmware first (if you have a model 575 or 59x server), and then the server firmware second.

Perform tasks 1 through 6 to obtain server firmware and power subsystem firmware updates (if you have a model 575 or 59x server).

Note: By default, the server firmware is installed on the temporary side only after the existing contents of the temporary side are permanently installed on the permanent side. (This process is performed automatically when you install a server firmware update.) If you want to preserve the contents of the permanent side, select **Install and Activate** from the Advanced Features on the HMC interface, and indicate that you do *not* want to automatically accept the firmware level.

Step 1. Ensure that you have an Internet connection:

To download updates from the service and support system or Web site to your HMC or server, you must have a connection to service and support either through a modem, direct or indirect Internet, or pass-through system.

To verify that the service connection is working, perform the following steps:

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using a an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
 - a. In the navigation area, open **Service Applications**.
 - b. Select **Remote Support**.
 - c. Select **Customize Outbound Connectivity**.
 - d. Continue with step 4 on page 142.
3. Perform the following steps:

- a. In the Navigation area, click **Service Management**.
- b. Select **Manage Outbound Connectivity**.
4. Select the tab for the type of outbound connectivity that you chose for your HMC (Local Modem, Internet VPN, or Pass-Through Systems). For more information about these settings, see Specifying the connection type from the HMC.

Note: If a connection to service and support does not exist, set up the service connection before proceeding with this procedure. For instructions on how to set up a connection to service and support, see Setting up your server to connect to service and support.

5. Click **Test**.
6. Verify that the test completes successfully. If the test is not successful, troubleshoot your connectivity and correct the problem before proceeding with this procedure. Alternatively, you can obtain the update on CD.
7. Continue with "Step 2. Review your HMC machine code version and release."

Step 2. Review your HMC machine code version and release:

The level of machine code on the HMC will determine the available features, including concurrent server firmware maintenance and enhancements to upgrading to a new release.

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
 - a. In the navigation area, open **Licensed Internal Code Maintenance**.
 - b. Select **HMC Code Update**.
 - c. In the contents area, view and record the version and release of your HMC machine code in the Status area.
 - d. Continue with 4.
3. Perform the following steps:
 - a. In the Navigation area, click **Updates**.
 - b. In the Work area, view and record the information that appears under the HMC Code Level heading, including: the HMC version, release, maintenance level, build level, and base versions.
4. Continue with "Step 3. View existing firmware levels with an HMC."

Step 3. View existing firmware levels with an HMC:

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 4 on page 143.
2. Ensure that the managed systems and power frames (if you have a model 575 or 59x server) are in the correct state.
 - a. From the HMC, select **Server and Partition**.
 - b. Select **Server Management** and ensure that the State is Power Off, Standby, or Operating.
 - c. If you have a model 575 or 59x server, select **Frame Management** and ensure that the state is Standby.
3. Perform the following steps:
 - a. From the HMC, expand the **Licensed Internal Code Maintenance** folder.
 - b. Click the **Licensed Internal Code Updates** icon.
 - c. Select **Change Licensed Internal Code for the current release**.

- d. 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 firmware level.
 - e. In the Change Licensed Internal Code window, select **View system information**, and click **OK**.
 - f. 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 firmware that has been installed and will be installed into memory after the managed system is powered off and powered on.
 - The *Activated Level* indicates the level of firmware that is active and running in memory.
 - The *Accepted Level* indicates the backup level of firmware. You can return to the backup level of firmware if you decide to remove the installed level.
 - g. Record the installed level and click **Close**.
 - h. Click **Cancel**.
 - i. Continue with step 5.
4. Perform the following steps:
 - a. In the Navigation area, click **Updates**.
 - b. Ensure that the managed system Status is Power Off, Standby, or Operating.
 - c. Record the level that appears in the EC Number field. For example, 01EM310.
 5. For information on compatible levels of HMC machine code and system firmware, refer to the POWER5 Code Matrix Web site.
 6. Choose from the following options:
 - If you need to update your HMC machine code, refer to Obtaining HMC machine code updates and upgrades.
 - If your HMC machine code is equal to or greater than the level of server firmware you want to install, continue with this procedure.
 7. Continue with "Step 4. View the available firmware levels."

Related concepts

"Obtaining HMC machine code updates and upgrades" on page 121
 Learn how to obtain HMC machine code updates and upgrades.

Step 4. View the available firmware levels:

To view the available levels, follow these steps:

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
 - a. From the HMC, expand the **Licensed Internal Code Maintenance** folder.
 - b. Click the **Licensed Internal Code Updates** icon.
 - c. In the Contents area, click **Change Internal Code for the current release**.
 - d. In the Target Object Selection window, click the target system, and click **OK**.
 - e. In the Change Internal Code window, select **View system information**.
 - f. Continue with step 4.
3. Perform the following steps:
 - a. In the Navigation area, click **Updates**.
 - b. Select the target system.
 - c. In the Task area, select **View system information**.
4. In the Specify LIC Repository window, select the repository location from which you want to view available firmware updates, and click **OK**. The following options are available:

- **IBM service Web site** (This site provides the most recent level of updates. You need a direct Internet connection to access this site.)
- **IBM support system** (This site provides all available levels of updates. You can use a modem or direct Internet connection to access this site.)
- **DVD-RAM media:** Select this option if you previously put the update on CD and it is in the DVD drive on the HMC.

Note: If you choose the DVD-RAM media repository and receive an I/O error when using a CD that you created, it might mean that the software you used to create the CD does not conform to the requirements for writing of temporary records on the HMC.

- **FTP site:** Select this option if you previously downloaded the update to an FTP site. (This site would be setup previously by your organization's advanced support personnel.) An FTP server is any system on which the FTP server protocol is activated. If you select the FTP site, you need to know the following information:

Note: Usually, a PC has only the FTP client active.

- **FTP site** - The fully qualified host and domain name of the FTP server from which you want to download the update.
- **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 or power subsystem firmware update. You can specify the default directory /opt/ccfw/data if you placed the update in that directory, or you can change the directory path if the update is in a directory other than the default directory. For example, if you downloaded the update and copied it to a unique directory on the FTP server, you can specify that directory.
- **Hard drive:** Select this option if you previously downloaded the update to the hard disk drive on your HMC. (This repository can be selected after a successful Code Update for this release was the last completed update to another Managed System or Power Subsystem by this HMC.)

Note: For more information about each of the repository locations, click **Help**.

A window is displayed that shows system information for the target system, including the retrievable levels of firmware. For details on retrievable levels of firmware, see Levels of firmware (Licensed Internal Code) on the HMC.

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

5. Record the available firmware level or levels.
6. Continue with "Step 5. Update a current release or upgrade to a new release."

Related concepts

"Available levels of server firmware and power subsystem firmware" on page 118

Step 5. Update a current release or upgrade to a new release:

Important: Do not interrupt the update or upgrade process once it begins.

Note: If you receive an error during the code update and are sent to the Service Focal Point application in the HMC, it means that you need to repair and close any open events that caused the code update to fail. For details, see Using Service Focal Point for the HMC. If you receive an HSCFxxxx reference code during the update, refer to the HSCFxxxx Licensed Internal Code error codes.

To update a current release or upgrade to a new release, follow these steps:

1. Note the following:

- You *must* install HMC updates before you install server firmware or power subsystem firmware updates so that the HMC can handle any updates or new function that you apply to the server.
 - If an HMC manages multiple servers at different firmware release levels, the HMC machine code level must be equal to or higher than the system firmware level on the server that is at the latest release level.
 - For instructions on how to update your HMC machine code, see Obtaining HMC machine code updates and upgrades.
 - After you install HMC updates, you should either install the power subsystem firmware and server firmware updates together, or install the power subsystem firmware first (if you have a model 575 or 59x server), and then the server firmware second.
2. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 3.
 - If you are using an HMC with Version 7 or later, continue with step 5.
 3. Ensure that the managed systems and power frames (if you have a model 575 or 59x server) are in the correct state.
 - a. From the HMC, select **Server and Partition**.
 - b. Select **Server Management** and ensure that the State is Power Off, Standby, or Operating.
 - c. If you have a model 575 or 59x server, select **Frame Management** and ensure that the state is Standby.
 4. Perform the following steps:
 - a. Expand the **Licensed Internal Code Maintenance** folder.
 - b. Click the **Licensed Internal Code Updates** icon.
 - c. Continue with step 6.
 5. Perform the following steps:
 - a. In the Navigation area, click **Updates**.
 - b. Select the target system.
 - c. Ensure that the status for the system is Power Off, Standby, or Operating.
 6. Choose from the following options:
 - To update a current release, continue with “Step 5.1. Update a current release.”
 - To upgrade to a new release, continue with “Step 5.2. Upgrade to a new release” on page 148.

Note: If you are unsure about whether to select an update or upgrade, select “Step 5.1. Update a current release.”

Related concepts

“Using Service Focal Point for the HMC” on page 436

Learn about using the Service Focal Point for the HMC to help you diagnose and repair problems on the system.

“Obtaining HMC machine code updates and upgrades” on page 121

Learn how to obtain HMC machine code updates and upgrades.

Related tasks

“HSCFxxx Licensed Internal Code error codes” on page 277

Step 5.1. Update a current release:

1. Select **Change Licensed Internal Code for the current release**.
2. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 3 on page 146.
 - If you are using an HMC with Version 7 or later, continue with step 4 on page 146.

3. In the Target Object Selection window, click the target system, and click **OK**. The target is the managed system for which you want to update.

Note: You can select multiple managed systems to be updated simultaneously. If you have a 575 system, there are some considerations you should review before choosing to update or upgrade multiple managed systems. For details, refer to Applying firmware to multiple managed systems using an HMC.

4. In the Change Licensed Internal Code window, select **Start Change Licensed Internal Code wizard** and click **OK**.
5. In the Specify LIC Repository window, select the repository location from which you want to download the server firmware or power subsystem firmware updates, and click **OK**. The following options are available:

- **IBM service Web site** (This site provides the most recent level of updates. You need a direct Internet connection to access this site.)
- **IBM support system** (This site provides all available levels of updates. You can use a modem or direct Internet connection to access this site.)

Note: Downloading server firmware or power subsystem firmware updates over a modem might take several hours.

- **DVD-RAM media:** Select this option if you previously put the update on CD and it is in the DVD drive on the HMC.

Note: If you choose the DVD-RAM media repository and receive an I/O error when using a CD that you created, it might mean that the software you used to create the CD does not conform to the requirements for writing of temporary records on the HMC.

- **FTP site:** Select this option if you previously downloaded the update to an FTP site. (This site would be set up previously by your organization's advanced support personnel.) An FTP server is any system on which the FTP server protocol is activated. If you select the FTP site, you need to know the following information:

Note: Usually, a PC has only the FTP client active.

- **FTP site** - The fully qualified host and domain name of the FTP server from which you want to download the update.
- **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 or power subsystem firmware update. You can specify the default directory `/opt/ccfw/data` if you placed the update in that directory, or you can change the directory path if the update is in a directory other than the default directory. For example, if you downloaded the update and copied it to a unique directory on the FTP server, you can specify that directory.
- **Hard drive:** Select this option if you previously downloaded the update to the hard disk drive on your HMC. (This repository can be selected after a successful Code Update for this release was the last completed update to another Managed System or Power Subsystem by this HMC, or the update was downloaded using the Retrieve function from the Advanced Features on the HMC interface.)

Note: For more information about each of the repository locations, click **Help**.

6. In the welcome window, click **Next**. One of the following will occur:
 - If the selected repository has only an update to the current release available, continue with step 7 on page 147.
 - If a message displays stating that there is a new upgrade level available, choose from the following options:

- Click **Cancel** to switch to an upgrade to a new release. You will *not* have to reselect the repository. Then continue with step 5 on page 149 in Step 5.2.
 - Click **OK** to proceed with an update for the current release, and continue with step 7.
 - If there are no updates or upgrades available for your current release, a message displays indicating that targets are up to date. In this situation, click **Cancel** to end the task.
7. In the Change Licensed Internal Code wizard window, ensure that **Managed System and Power LIC** is selected and choose from the following options:
- If the window contains a grayed out message across from 'Current Installation type selection' continue with step 8.
 - If the window contains a message regarding the availability of a concurrent update across from 'Current Installation type selection' choose from the following options:
 - To continue with a concurrent update, follow these steps:
 - a. Read the message that is displayed.
 Notice: Do not perform any configuration or management operations on the managed system while Licensed Internal Code is being updated.
- Notes:**
- Do not perform any tasks on the managed system that is being updated until the firmware update is complete.
 - If an operation does occur, both the code update and operation might complete correctly.
 - However, if there is a failure, allow the update to complete before retrying a new operation.
 - If the concurrent firmware update fails, remove the corrupted image and retry the concurrent Licensed Internal Code update. For details, see Removing the current firmware level.
- b. Continue with step 8.
 - To change to disruptively install and activate the update, click **Advanced Options**.
 - a. In the Concurrency window, select the target that you want to update. The type of installation is shown in the Concurrency Status field.
 - b. In the Select the type of installation to perform area, choose from the available options, which might include:
 - Concurrent install and activate
 - Concurrent only, with deferred disruptive activate
 - Disruptive install and activate
 - c. Click **OK** and continue with step 8.
8. Click **Next**. The Hardware Management Console License Agreement window is displayed.
9. In the 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 following message is displayed on the HMC interface, you will need to manually shut down all of the applications and logical partitions to prevent the system from shutting them down abnormally during the process. Quiesce any applications currently running on your operating systems for the systems listed below.
- Perform the following steps:
- a. Use the usual procedures to shut down the logical partitions:
 - To shut down AIX logical partitions, see Shutting down AIX logical partitions.

- To shut down i5/OS logical partitions, use the Power Down System (PWRDWN SYS RESTART *NO) command from an i5/OS command line (either in a 5250 emulator session on your HMC, or on the Operations Console). For further details, see Shutting down i5/OS logical partitions.
 - To shut down Linux logical partitions, see Shutting down Linux logical partitions.
- b. Power off the managed system.
 - c. Restart the HMC after the server is off.
 - d. Use the Change Licensed Internal Code Wizard to apply the firmware. Do not interrupt this process.
 - e. Restart the managed system.
 - f. Activate the Logical Partitions.

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

11. To verify that the update installed correctly, see “Step 6. Verify that the update installed correctly” on page 150.

Related concepts

“Applying firmware to multiple managed systems using an HMC” on page 120

Learn more about applying firmware to multiple managed systems using an HMC.

“Obtaining HMC machine code updates and upgrades” on page 121

Learn how to obtain HMC machine code updates and upgrades.

Related information

Shutting down AIX logical partitions

 Power Down System (PWRDWN SYS)

Shutting down i5/OS logical partitions

Shutting down Linux logical partitions

Step 5.2. Upgrade to a new release:

1. To upgrade to a new release, click **Upgrade Licensed Internal Code to a new release**.
2. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 3.
 - If you are using an HMC with Version 7 or later, continue with step 4.
3. 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 firmware to a new release.

Note: You can select multiple managed systems to be updated simultaneously (unless the DVD repository is used during an *upgrade*, then the upgrade will be performed sequentially). Also, if you have a 575 system, there are some considerations you should review before choosing to update or upgrade multiple managed systems. For details on using the DVD repository during an upgrade, or for considerations when updating or upgrading a 575 system, refer to Applying firmware to multiple managed systems using an HMC.

4. In the Specify LIC Repository window, select the repository location from which you want to download the server firmware or power subsystem firmware updates, and click **OK**.

Note: If you receive a message that you can only use the DVD-RAM media repository, it means that you do not have the correct HMC machine code release installed. You will need to update your HMC machine code before you continue. For details, see Obtaining HMC machine code updates and upgrades.

The following options are available:

- **IBM service Web site** (This site provides the most recent level of updates. You need a direct Internet connection to access this site.)

- **IBM support system** (This site provides all available levels of updates. You can use a modem or direct Internet connection to access this site.)

Note: Downloading server firmware or power subsystem firmware updates over a modem might take several hours.

- **DVD-RAM media:** Select this option if you previously put the update on CD and it is in the DVD drive on the HMC.

Note: If you choose the DVD-RAM media repository and receive an I/O error when using a CD that you created, it might mean that the software you used to create the CD does not conform to the requirements for writing of temporary records on the HMC.

Note: If you selected to upgrade multiple managed systems, the DVD-RAM media repository will perform the upgrade sequentially. For details, refer to Applying firmware to multiple managed systems using an HMC.

- **FTP site:** Select this option if you previously downloaded the update to an FTP site. (This site would be setup previously by your organization's advanced support personnel.) An FTP server is any system on which the FTP server protocol is activated. If you select the FTP site, you need to know the following information:

Note: Usually, a PC has only the FTP client active.

- **FTP site** - The fully qualified host and domain name of the FTP server from which you want to download the update.
- **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 or power subsystem firmware update. You can specify the default directory /opt/ccfw/data if you placed the update in that directory, or you can change the directory path if the update is in a directory other than the default directory. For example, if you downloaded the update and copied it to a unique directory on the FTP server, you can specify that directory.

5. In the License Agreement window, read the agreement and click **Accept**.
6. In the Confirm the Action window, perform the required actions, and click **Finish**.

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

Perform the following steps:

- a. Use the usual procedures to shut down the logical partitions:
 - To shut down AIX logical partitions, see Shutting down AIX logical partitions.
 - To shut down i5/OS logical partitions, use the Power Down System (PWRDWN SYS RESTART *NO) command from an i5/OS command line (either in a 5250 emulator session on your HMC, or on the Operations Console). For further details, see Shutting down i5/OS logical partitions.
 - To shut down Linux logical partitions, see Shutting down Linux logical partitions.
- b. Power off the managed system.
- c. Restart the HMC after the server is off.
- d. Use the Change Licensed Internal Code Wizard to apply the firmware. Do not interrupt this process.
- e. Restart the managed system.
- f. Activate the Logical Partitions.

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

7. To verify that the update installed correctly, continue with “Step 6. Verify that the update installed correctly.”

Related concepts

“Applying firmware to multiple managed systems using an HMC” on page 120

Learn more about applying firmware to multiple managed systems using an HMC.

“Obtaining HMC machine code updates and upgrades” on page 121

Learn how to obtain HMC machine code updates and upgrades.

Related information

Shutting down AIX logical partitions

 Power Down System (PWRDWN SYS)

Shutting down i5/OS logical partitions

Shutting down Linux logical partitions

Step 6. Verify that the update installed correctly:

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 4 on page 143.
2. Ensure that the managed systems and power frames (if you have a model 575 or 59x server) are in the correct state.
 - a. From the HMC, select **Server and Partition**.
 - b. Select **Server Management** and ensure that the State is Power Off, Standby, or Operating.
 - c. If you have a model 575 or 59x server, select **Frame Management** and ensure that the state is Standby.
3. Perform the following steps:
 - a. In the navigation area, expand the **Licensed Internal Code Maintenance** folder.
 - b. Click the **Licensed Internal Code Updates** icon.
 - c. Select **Change Licensed Internal Code for the current release**.
 - d. 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 firmware level.
 - e. In the Change Licensed Internal Code window, select **View system information**, and click **OK**.
 - f. 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 firmware that has been installed and will be installed into memory after the managed system is powered off and powered on.
 - The *Activated Level* indicates the level of firmware that is active and running in memory.
 - The *Accepted Level* indicates the backup level of firmware. You can return to the backup level of firmware if you decide to remove the installed level.
 - g. Record the installed level and click **Close**.
 - h. Click **Cancel**.
 - i. Continue with step 5.
4. Perform the following steps:
 - a. In the Navigation area, click **Updates**.
 - b. Ensure that the managed system Status is Power Off, Standby, or Operating.
 - c. Record the level that appears in the EC Number field. For example, 01EM310.
5. If the level of firmware does not match the update that you installed, perform the following steps:
 - a. Check the network connection on the HMC.
 - b. Retry the update using a different repository.

- c. If the problem persists, contact your next level of support.

Obtaining firmware updates through an HMC using a CD, FTP server, or hard drive:

Learn how to update or upgrade server firmware and power subsystem firmware (if you have a model 575 or 59x server) through an HMC using a CD, FTP server, a hard drive to apply the update.

Important: The HMC machine code needs to be equal to or greater than the server firmware level. Also, if an HMC manages multiple servers at different firmware release levels, the HMC machine code level must be equal to or higher than the system firmware level on the server that is at the latest release level. During this procedure you will find out how to ensure your HMC machine code and server firmware is compatible.

You *must* install HMC updates before you install server firmware or power subsystem firmware updates so that the HMC can handle any updates or new function that you apply to the server. After you install HMC updates, either install the power subsystem firmware and server firmware updates together, or install the power subsystem firmware first (if you have a model 575 or 59x server), and then the server firmware second.

Perform tasks 1 through 5 to obtain server firmware and power subsystem firmware updates (if you have a model 575 or 59x server).

Note: By default, the server firmware is installed on the temporary side only after the existing contents of the temporary side are permanently installed on the permanent side. (This process is performed automatically when you install a server firmware update.) If you want to preserve the contents of the permanent side, select **Install and Activate** from the Advanced Features on the HMC interface, and indicate that you do *not* want to automatically accept the firmware level.

Step 1. Review your HMC machine code version and release:

The level of machine code on the HMC will determine the available features, including concurrent server firmware maintenance and enhancements to upgrading to a new release.

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
 - a. In the navigation area, open **Licensed Internal Code Maintenance**.
 - b. Select **HMC Code Update**.
 - c. In the contents area, view and record the version and release of your HMC machine code in the Status area.
 - d. Continue with 4.
3. Perform the following steps:
 - a. In the Navigation area, click **Updates**.
 - b. In the Work area, view and record the information that appears under the HMC Code Level heading, including: the HMC version, release, maintenance level, build level, and base versions.
4. Continue with "Step 2. View existing firmware levels with an HMC."

Step 2. View existing firmware levels with an HMC:

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2 on page 152.
 - If you are using an HMC with Version 7 or later, continue with step 4 on page 152.

2. Ensure that the managed systems and power frames (if you have a model 575 or 59x server) are in the correct state.
 - a. From the HMC, select **Server and Partition**.
 - b. Select **Server Management** and ensure that the State is Power Off, Standby, or Operating.
 - c. If you have a model 575 or 59x server, select **Frame Management** and ensure that the state is Standby.
3. Perform the following steps:
 - a. From the HMC, expand the **Licensed Internal Code Maintenance** folder.
 - b. Click the **Licensed Internal Code Updates** icon.
 - c. Select **Change Licensed Internal Code for the current release**.
 - d. 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 firmware level.
 - e. In the Change Licensed Internal Code window, select **View system information**, and click **OK**.
 - f. 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 firmware that has been installed and will be installed into memory after the managed system is powered off and powered on.
 - The *Activated Level* indicates the level of firmware that is active and running in memory.
 - The *Accepted Level* indicates the backup level of firmware. You can return to the backup level of firmware if you decide to remove the installed level.
 - g. Record the installed level and click **Close**.
 - h. Click **Cancel**.
 - i. Continue with step 5.
4. Perform the following steps:
 - a. In the Navigation area, click **Updates**.
 - b. Ensure that the managed system Status is Power Off, Standby, or Operating.
 - c. Record the level that appears in the EC Number field. For example, 01EM310.
5. For information on compatible levels of HMC machine code and system firmware, refer to the POWER5 Code Matrix Web site.
6. Choose from the following options:
 - If you need to update your HMC machine code, refer to Obtaining HMC machine code updates and upgrades.
 - If your HMC machine code is equal to or greater than the level of server firmware you want to install, continue with this procedure.

Related concepts

“Obtaining HMC machine code updates and upgrades” on page 121
 Learn how to obtain HMC machine code updates and upgrades.


Related information

 POWER5 Code Matrix Web site

Step 3. View or download the firmware update:

To view or download the server firmware and power subsystem firmware updates, follow these steps:

Note: If you plan to create a CD, you will need a CD burner and software. If you prefer to order an update CD, contact service and support (AIX or Linux), or use the Fix Central Web site (i5/OS).

1. From a computer or server with an Internet connection, go to the Fix Central Web site at <http://www.ibm.com/eserver/support/fixes/> .

2. Select the appropriate family in the Product family list.
3. Choose from the following options:
 - For AIX or Linux, continue with step 4.
 - For i5/OS, continue with step 7.
4. For AIX or Linux, perform the following steps:
 - a. From the Fix Central Web site, select **Hardware microcode and firmware** in the Product or fix type list.
 - b. Click **Continue**.
 - c. Select your machine type and model from the drop-down list. An information window is displayed.
5. To download the ISO image, perform the following steps:
 - a. Click **Desc**. An HTML file is displayed.
 - b. In the Description file, click the .ISO file. For example, or SF2aa_bbb_BP2cc_ddd.iso.
 - c. Follow the on-screen prompts.
 - d. If you want to create a CD, follow the instructions for your CD program and then continue with "Step 4. Update a current release or upgrade to a new release" on page 154.
6. To download the firmware RPM and XML files, perform the following steps:
 - a. Select the **RPM** check box for the server firmware version you want.
 - b. If you have a model 575 or 59x server, select the **RPM** check box for the power subsystem firmware version that corresponds to the system firmware you are installing.
 - c. Scroll to the bottom of the page and click **Continue**.
 - d. Click **Continue** again. The License Agreement is displayed.
 - e. Click **I agree to abide by its terms** and click **Continue**.
 - f. Follow the on-screen prompts. You will need to select the XML file when prompted to apply the firmware through the HMC.
 - g. If you want to create a CD, follow the instructions for your CD program and then continue with "Step 4. Update a current release or upgrade to a new release" on page 154.
7. For i5/OS, perform the following steps:

Note: This selection includes both server firmware and power subsystem firmware (if you have a model 575 or 59x).

- b. Select **Update policy set to HMC** in the Firmware update policy.
- c. Click **Continue**.
- d. Click **Recommended fixes** on the Server firmware fixes page.
- e. From the Recommended fixes page, select your version and release in the Select your release field (for example, V5R3).
- f. Select **Server Firmware: Update Policy Set to HMC** from the select a topic list.
- g. Click **Go**.
- h. Record the available firmware.
- i. If you want to download or order the firmware, choose from the following options:
 - To download the ISO image which contains both the server firmware and power subsystem firmware (if you have a model 575 or 59x server), click **Go** across from the .iso image.
 - To download the RPM and XML files, click Download.rpm Download.xml for server firmware files and Bulk power files (if you have a model 575 or 59x server).
 - To order the update on CD, click the MHxxxxx file. You will be prompted for your IBM ID and Password.

Note: In the following screens, you will need to select both of the following to receive the CD:

- Immediate download over the Internet (HTTP)
- Mail order on CD if the total size exceeds the limits you selected above

Note: You also can order the CD using the SNDPTFORD command.

- j. Follow the on-screen prompts.
- k. If you want to create a CD, follow the instructions for your CD program and then continue with “Step 4. Update a current release or upgrade to a new release.”

Step 4. Update a current release or upgrade to a new release:

Important: Do not interrupt the update or upgrade process once it begins.

Note: If you receive an error during the code update and are sent to the Service Focal Point application in the HMC, it means that you need to repair and close any open events that caused the code update to fail. For details, see Using Service Focal Point for the HMC. If you receive an HSCFxxxx reference code during the update, refer to the HSCFxxxx Licensed Internal Code error codes.

To update a current release or upgrade to a new release, follow these steps:

1. Note the following:
 - You *must* install HMC updates before you install server firmware or power subsystem firmware updates so that the HMC can handle any updates or new function that you apply to the server.
 - If an HMC manages multiple servers at different firmware release levels, the HMC machine code level must be equal to or higher than the system firmware level on the server that is at the latest release level.
 - For instructions on how to update your HMC machine code, see Obtaining HMC machine code updates and upgrades.
 - After you install HMC updates, you should either install the power subsystem firmware and server firmware updates together, or install the power subsystem firmware first (if you have a model 575 or 59x server), and then the server firmware second.
2. If you obtained an update CD for this procedure, insert it into the CD drive on the HMC.
3. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 4.
 - If you are using an HMC with Version 7 or later, continue with step 6.
4. Ensure that the managed systems and power frames (if you have a model 575 or 59x server) are in the correct state.
 - a. From the HMC, select **Server and Partition**.
 - b. Select **Server Management** and ensure that the State is Power Off, Standby, or Operating.
 - c. If you have a model 575 or 59x server, select **Frame Management** and ensure that the state is Standby.
5. Perform the following steps:
 - a. From the HMC, expand the **Licensed Internal Code Maintenance** folder.
 - b. Click the **Licensed Internal Code Updates** icon.
 - c. Continue with step 7.
6. Perform the following steps:
 - a. In the Navigation area, click **Updates**.
 - b. Select the target system.
 - c. Ensure that the status for the system is Power Off, Standby, or Operating.
7. Choose from the following options:

- To update a current release, continue with “Step 4.1. Update a current release.”
- To upgrade to a new release, go to “Step 4.2. Upgrade to a new release” on page 157.

Note: If you are unsure, select “Step 4.1. Update a current release.”

Related concepts

“Using Service Focal Point for the HMC” on page 436

Learn about using the Service Focal Point for the HMC to help you diagnose and repair problems on the system.

Related tasks

“HSCFxxxx Licensed Internal Code error codes” on page 277

Step 4.1. Update a current release:

1. Select **Change Licensed Internal Code for the current release**.
2. In the Target Object Selection window, click the target system, and click **OK**. The target is the managed system for which you want to update.

Note: You can select multiple managed systems to be updated simultaneously. If you have a 575 system, there are some considerations you should review before choosing to update or upgrade multiple managed systems. For details, refer to Applying firmware to multiple managed systems using an HMC.

3. In the Change Licensed Internal Code window, select **Start Change Licensed Internal Code wizard** and click **OK**.
4. In the Specify LIC Repository window, select the repository location from which you want to download the server firmware or power subsystem firmware updates, and click **OK**. The following options are available:
 - **IBM service Web site** (This site provides the most recent level of updates. You need a direct Internet connection to access this site.)
 - **IBM support system** (This site provides all available levels of updates. You can use a modem or direct Internet connection to access this site.)

Note: Downloading server firmware or power subsystem firmware updates over a modem might take several hours.

- **DVD-RAM media:** Select this option if you previously put the update on CD and it is in the DVD drive on the HMC.

Note: If you choose the DVD-RAM media repository and receive an I/O error when using a CD that you created, it might mean that the software you used to create the CD does not conform to the requirements for writing of temporary records on the HMC.

- **FTP site:** Select this option if you previously downloaded the update to an FTP site. (This site would be set up previously by your organization’s advanced support personnel.) An FTP server is any system on which the FTP server protocol is activated. If you select the FTP site, you need to know the following information:

Note: Usually, a PC has only the FTP client active.

- **FTP site** - The fully qualified host and domain name of the FTP server from which you want to download the update.
- **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 or power subsystem firmware update. You can specify the default directory `/opt/ccfw/data` if you placed the update in that directory, or you can change the directory path if the update is in a directory other than the

default directory. For example, if you downloaded the update and copied it to a unique directory on the FTP server, you can specify that directory.

- **Hard drive:** Select this option if you previously downloaded the update to the hard disk drive on your HMC. (This repository can be selected after a successful Code Update for this release was the last completed update to another Managed System or Power Subsystem by this HMC, or the update was downloaded using the Retrieve function from the Advanced Features on the HMC interface.)

Note: For more information about each of the repository locations, click **Help**.

5. In the welcome window, click **Next**. One of the following will occur:
 - If the selected repository has only an update to the current release available, continue with step 6.
 - If a message displays stating that there is a new upgrade level available, choose from the following options:
 - Click **Cancel** to switch to an upgrade to a new release. You will *not* have to re-select the repository. Then continue with step 4 on page 158 in Step 5.2.
 - Click **OK** to proceed with an update for the current release, and continue with step 6.
 - If no change updates are available, a message displays indicating that no updates are available and targets are up to date. In this situation, click **Cancel** to end the task.
6. In the Change Licensed Internal Code wizard window, ensure that **Managed System and Power LIC** is selected and choose from the following options:
 - If the window contains a grayed out message across from 'Current Installation type selection' continue with step 7.
 - If the window contains a concurrent message across from 'Current Installation type selection' choose from the following options:
 - To continue with a concurrent update, follow these steps:
 - a. Read the message that is displayed.

Notice: Do not perform any configuration or management operations on the managed system while Licensed Internal Code is being updated.
 - Note:** Do not perform any tasks on the managed system that is being updated until the firmware update is complete. If an operation does occur, both the code update and operation might complete correctly. However, if there is a failure, allow the update to complete before retrying a new operation. If the concurrent firmware update fails, remove the corrupted image and retry the concurrent update. For details, see Removing the current firmware level.
 - b. Continue with step 7.
 - To change to a disruptive install and activate, click **Advanced Options**.
 - a. In the Concurrency window, select the target you want to update. The type of installation is shown in the Concurrency Status field.
 - b. In the Select the type of installation to perform area, choose from the available options, which might include:
 - Concurrent install and activate
 - Concurrent only, with deferred disruptive activate
 - Disruptive install and activate
 - c. Click **OK** and continue with step 7.
7. Click **Next**. The Hardware Management Console License Agreement window is displayed.
8. In the License Agreement window, read the agreement and click **Accept**.

9. In the Confirm the Action window, perform the required actions, and click **Finish**.

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

Perform the following steps:

- a. Use the usual procedures to shut down the logical partitions:
 - To shut down AIX logical partitions, see Shutting down AIX logical partitions.
 - To shut down i5/OS logical partitions, use the Power Down System (PWRDWNSYS RESTART *NO) command from an i5/OS command line (either in a 5250 emulator session on your HMC, or on the Operations Console). For further details, see Shutting down i5/OS logical partitions.
 - To shut down Linux logical partitions, see Shutting down Linux logical partitions.
- b. Power off the managed system.
- c. Restart the HMC after the server is off.
- d. Use the Change Licensed Internal Code Wizard to apply the firmware. Do not interrupt this process.
- e. Restart the managed system.
- f. Activate the Logical Partitions.

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

10. To verify that the update installed correctly, see “Step 5. Verify that the update installed correctly” on page 159.

Related concepts

“Applying firmware to multiple managed systems using an HMC” on page 120

Learn more about applying firmware to multiple managed systems using an HMC.

Related tasks

“Removing the current firmware level” on page 195

Find out how to remove the current level of firmware so you can return to a previous level of server firmware or power subsystem firmware.

Related information

Shutting down AIX logical partitions

 Power Down System (PWRDWNSYS)

Shutting down i5/OS logical partitions

Shutting down Linux logical partitions

Step 4.2. Upgrade to a new release:

1. To upgrade to a new release, click **Upgrade Licensed Internal Code to a new release**.
2. 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 firmware to a new release.

Note: You can select multiple managed systems to be updated simultaneously (unless the DVD repository is used during an *upgrade*, then the upgrade will be performed sequentially). Also, if you have a 575 system, there are some considerations you should review before choosing to update or upgrade multiple managed systems. For details on using the DVD repository during an upgrade, or for considerations when updating or upgrading a 575 system, refer to Applying firmware to multiple managed systems using an HMC.

3. In the Specify LIC Repository window, select the repository location from which you want to download the server firmware or power subsystem firmware updates, and click **OK**.

Note: If you receive a message that you can only use the DVD-RAM media repository, it means that you do not have the correct HMC machine code release installed. You will need to update your HMC machine code before you continue. For details, see Obtaining HMC machine code updates and upgrades.

The following options are available:

- **IBM service Web site** (This site provides the most recent level of updates. You need a direct Internet connection to access this site.)
- **IBM support system** (This site provides all available levels of updates. You can use a modem or direct Internet connection to access this site.)

Note: Downloading server firmware or power subsystem firmware updates over a modem might take several hours.

- **DVD-RAM media:** Select this option if you previously put the update on CD and it is in the DVD drive on the HMC.

Note: If you choose the DVD-RAM media repository and receive an I/O error when using a CD that you created, it might mean that the software you used to create the CD does not conform to the requirements for writing of temporary records on the HMC.

Note: If you selected to upgrade multiple managed systems, the DVD-RAM media repository will perform the upgrade sequentially. For details, refer to Applying firmware to multiple managed systems using an HMC.

- **FTP site:** Select this option if you previously downloaded the update to an FTP site. (This site would be setup previously by your organization's advanced support personnel.) An FTP server is any system on which the FTP server protocol is activated. If you select the FTP site, you need to know the following information:

Note: Usually, a PC has only the FTP client active.

- **FTP site** - The fully qualified host and domain name of the FTP server from which you want to download the update.
- **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 or power subsystem firmware update. You can specify the default directory /opt/ccfw/data if you placed the update in that directory, or you can change the directory path if the update is in a directory other than the default directory. For example, if you downloaded the update and copied it to a unique directory on the FTP server, you can specify that directory.

4. In the License Agreement window, read the agreement and click **Accept**.
5. In the Confirm the Action window, perform the required actions, and click **Finish**.

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

Perform the following steps:

- a. Use the usual procedures to shut down the logical partitions:
 - To shut down AIX logical partitions, see Shutting down AIX logical partitions.
 - To shut down i5/OS logical partitions, use the Power Down System (PWRDWN SYS RESTART *NO) command from an i5/OS command line (either in a 5250 emulator session on your HMC, or on the Operations Console). For further details, see Shutting down i5/OS logical partitions.
 - To shut down Linux logical partitions, see Shutting down Linux logical partitions.
- b. Power off the managed system.

- c. Restart the HMC after the server is off.
- d. Use the Change Licensed Internal Code Wizard to apply the firmware. Do not interrupt this process.
- e. Restart the managed system.
- f. Activate the Logical Partitions.

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

6. To verify that the update installed correctly, see “Step 5. Verify that the update installed correctly.”

Related concepts

“Applying firmware to multiple managed systems using an HMC” on page 120

Learn more about applying firmware to multiple managed systems using an HMC.

“Obtaining HMC machine code updates and upgrades” on page 121

Learn how to obtain HMC machine code updates and upgrades.

Related information

Shutting down AIX logical partitions

 Power Down System (PWRDWN SYS)

Shutting down i5/OS logical partitions

Shutting down Linux logical partitions

Step 5. Verify that the update installed correctly:

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 4.
2. Ensure that the managed systems and power frames (if you have a model 575 or 59x server) are in the correct state.
 - a. From the HMC, select **Server and Partition**.
 - b. Select **Server Management** and ensure that the State is Power Off, Standby, or Operating.
 - c. If you have a model 575 or 59x server, select **Frame Management** and ensure that the state is Standby.
3. Perform the following steps:
 - a. From the HMC, expand the **Licensed Internal Code Maintenance** folder.
 - b. Click the **Licensed Internal Code Updates** icon.
 - c. Select **Change Licensed Internal Code for the current release**.
 - d. 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 firmware level.
 - e. In the Change Licensed Internal Code window, select **View system information**, and click **OK**.
 - f. 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 firmware that has been installed and will be installed into memory after the managed system is powered off and powered on.
 - The *Activated Level* indicates the level of firmware that is active and running in memory.
 - The *Accepted Level* indicates the backup level of firmware. You can return to the backup level of firmware if you decide to remove the installed level.
 - g. Record the installed level and click **Close**.
 - h. Click **Cancel**.
 - i. Continue with step 5 on page 160.
4. Perform the following steps:

- a. In the Navigation area, click **Updates**.
 - b. Ensure that the managed system Status is Power Off, Standby, or Operating.
 - c. Record the level that appears in the EC Number field. For example, 01EM310.
5. If the level of firmware does not match the update that you installed, perform the following steps:
 - a. Retry the machine code update. If you created a CD or DVD for this procedure, use a new media.
 - b. If the problem persists, contact your next level of support.

Obtaining server firmware updates through AIX or Linux without an HMC:

Learn how to obtain updates to server firmware through AIX or Linux without an HMC.

Installing server firmware updates through the operating system is a disruptive process.

Note: If you have an IBM System i5® or eServer i5, you must either apply server firmware through an HMC or through an i5/OS logical partition.

Perform Steps 1 through 6 to get server firmware updates through AIX or Linux when you do not have an HMC.

Note: By default, the server firmware is installed on the temporary side only after the existing contents of the temporary side are permanently installed on the permanent side. (This process is performed automatically when you install a server firmware update.)

Note: If you are unable to start your AIX or Linux operating system or server, refer to “Obtaining server firmware updates through AIX or Linux when you are unable to start the operating system or server” on page 202.

Related tasks

“Obtaining server firmware updates through AIX or Linux when you are unable to start the operating system or server” on page 202

Learn how to apply server firmware updates through AIX or Linux when you are unable to start the operating system or server.

Step 1. View existing firmware levels for AIX or Linux:

1. Choose from the following options:
 - To use the ASMI (AIX or Linux): On the ASMI Welcome pane, view the existing level of server firmware in the upper-right corner below the copyright statement, for example, SF220_006.
 - To use the AIX command prompt (you must have AIX diagnostics installed on your server), continue with step 2.
 - To use the Linux command prompt, continue with step 4 on page 161.
2. At an AIX command prompt, enter the following command:

```
lsmcode
```

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

```
The current permanent system firmware image is SF220_005.
The current temporary system firmware image is SF220_006.
The system is currently booted from the temporary image.
```

Note:

- a. The permanent level is also known as the backup level.
- b. The temporary level is also known as the installed level.
- c. The system was booted from the temporary side, so at this time the temporary level is also the activated level.

3. Continue with “Step 2. View or download the firmware update.”
4. To view existing levels of server firmware for Linux, you must have the following service tools installed on 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.

Note: If you do not have the service tools on your server, refer to “Obtaining service and productivity tools for Linux” on page 207.

5. After the service tools are installed on the server running Linux, enter the following at a Linux command prompt:

```
lsmlcode
```

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

```
Version of system firmware is: 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.	The backup level.	The activated level.
Also known as the temporary level.	Also known as the permanent level.	The level on which the server is currently running.

6. Continue with “Step 2. View or download the firmware update.”


Related tasks

“Obtaining service and productivity tools for Linux” on page 207
Find out about obtaining service and productivity tools for Linux.

Step 2. View or download the firmware update:

Follow this procedure to view or download the firmware update. You can download the update directly to your server, or you can download it to a computer with an Internet connection and create an update CD that you apply on the server. If necessary, contact service and support to order the update on CD.

Note: If you plan to create a CD, you will need a CD burner and software. If you prefer to order an update CD, contact service and support.

1. From a computer or server with an Internet connection, go to the Fix Central Web site at <http://www.ibm.com/eserver/support/fixes/> .
2. Select **UNIX servers** in the Product family list.
3. Select **Hardware microcode and firmware** in the Product list.
4. Click **Continue**.
5. Perform the following steps:
 - a. Select your machine type and model from the drop-down list. An information window is displayed.
 - b. Click **Continue**. The available firmware levels are displayed.
 - c. Record the available firmware.

- d. If you want to download the update, choose from the following options:
 - To download the ISO image, continue with step 6.
 - To download the RPM file, continue with step 7.
6. To download the ISO image, follow these steps:
 - a. Click **Desc**. An HTML file appears.
 - b. In the Description file, click the .ISO file. For example, SF2aa_bbb_BP2cc_ddd.iso.

Note: If the ISO image is unavailable you will need to get the RPM file. Continue with step 7.

 - c. Follow the on-screen prompts.
 - d. Follow the instructions for your CD program to create a CD. Then go to “Step 3. View and unpack the RPM file that contains the server firmware.”
7. To download the RPM file, follow these steps:
 - a. Select the RPM check box for the server firmware version you want.
 - b. Scroll to the bottom of the page and click **Continue**.
 - c. Click **Continue** again. The License Agreement is displayed.
 - d. Click **I agree to abide by its terms** and click **Continue**.
 - e. Follow the on-screen prompts.
8. Choose from the following options:
 - If you downloaded the RPM file to your server, continue with “Step 3. View and unpack the RPM file that contains the server firmware.”
 - If you want to create a CD containing the RPM file, follow the instructions for your CD program and then continue with “Step 3. View and unpack the RPM file that contains the server firmware.”

Step 3. View and unpack the RPM file that contains the server firmware:

If you created a CD with the ISO image, or either downloaded or created a CD with the RPM file, you will need to view and unpack the RPM file that contains the server firmware.

1. Choose from the following options:
 - If you created a CD with the ISO image or the RPM file, continue with step 2.
 - If you downloaded the RPM file to your system, continue with step 6 on page 163.
2. Insert the CD that contains the .iso image or the RPM file into the media drive on your server.
3. To mount the CD, choose from the following options (you will need to have root user authority):
 - If you are working on an AIX system, enter the following at an AIX command prompt:
`mount /dev/cd0 /mnt`
 - If you are working on a Linux system, enter one of the following commands at a Linux command prompt:
`mount -t iso9660 /dev/cdrom /mnt`
or
`mount -t iso9660 /dev/dvdrom /mnt`
4. Choose from the following options:
 - If the mount was successful, continue with step 6 on page 163.
 - If the mount was unsuccessful, continue with the next step.
5. If you received the message, mount: 0506-324 Cannot mount /dev/cd0 on /mnt, perform the steps below to mount the CD:
 - a. Enter the command:
`/usr/sbin/mount -v 'cdrfs' -f'' -p'' -r'' /dev/cd0 /mnt`

The quotation marks following the *f*, *p*, and *r* are two single quotation marks with no space between them.

Note: If you prefer to use the System Management Interface Tool (SMIT) to mount the CD, see “Using the System Management Interface Tool to mount the update CD for AIX” on page 206.

- b. Continue with the next step.
6. To view the RPM file name, enter the following command at the AIX or Linux command prompt:
 - If the RPM file is on CD, type:
`ls /mnt`
 - If the RPM file is on the server, type:
`ls /tmp/fwupdate`The name of the RPM file is displayed. For example, you might see output similar to the following:
`01SF2xx_yyy_zzz.rpm`
7. To unpack the RPM file, enter one of the following commands at the AIX or Linux command prompt:
 - If you want to unpack from a CD, enter:
`rpm -Uvh --ignoreos /mnt/filename.rpm`
 - If you want to unpack from the server’s hard drive, enter:
`rpm -Uvh --ignoreos /tmp/fwupdate/filename.rpm`where *filename* is the name of the RPM file that contains the server firmware. For example,
`01SF2xx_yyy_zzz.rpm`.

Note: When you unpack the RPM file, the server firmware update file is saved in the `/tmp/fwupdate` directory on the server’s hard drive in the following format: `01SF2xx_yyy_zzz`.

8. Continue with “Step 4. Apply server firmware updates through AIX or Linux to the temporary side of the service processor.”

Related tasks

“Using the System Management Interface Tool to mount the update CD for AIX” on page 206
Use this procedure if you want to use SMIT to mount the update CD for AIX.

Step 4. Apply server firmware updates through AIX or Linux to the temporary side of the service processor:

Important: Do not interrupt this process once you begin.

1. Do you have a model 575 or 59x server?
 - **No:** Continue with the next step.
 - **Yes:** You must use the HMC to install server firmware updates. Refer to one of these procedures:
 - Obtaining server firmware and power subsystem firmware updates through an HMC with an Internet connection.
 - Obtaining server firmware and power subsystem firmware updates through an HMC using a CD, FTP server, or hard drive.
2. Is your AIX or Linux system or logical partition, IBM System p5, IBM eServer p5, or OpenPower® system managed by an HMC?
 - **No:** Continue with the next step.
 - **Yes:** You must use the HMC to apply the fix. Refer to one of these procedures:
 - Obtaining server firmware and power subsystem firmware updates through an HMC with an Internet connection.
 - Obtaining server firmware and power subsystem firmware updates through an HMC using a CD, FTP server, or hard drive.
3. Do you have a IBM System i5 or eServer i5?
 - **No:** Continue with the next step.

- **Yes:** You must apply the update through i5/OS or an HMC. Refer to one of the following procedures:
 - Obtaining server firmware updates through IBM i5/OS.
 - Obtaining server and power subsystem firmware updates through an HMC with an Internet connection.
 - Obtaining server firmware and power subsystem firmware updates through an HMC using a CD, FTP server, or hard drive.
- 4. Ensure you are starting the system from the temporary side of the service processor; the firmware installation will fail if the system has booted from the permanent side. To learn which side you are starting from, and how to change to the other side if necessary, refer to “Working with the temporary and permanent side of the service processor” on page 208.
- 5. To use the `update_flash` command (AIX or Linux) to install the server firmware, continue with step 6.

Note: If you have AIX installed, and prefer to use the AIX diagnostics to install the update, see “Using the AIX diagnostics to install the server firmware update through AIX” on page 204. If you plan to install the fix from CD, you will need to obtain the *Microcode Updates Files & Discovery Tool* CD to use the AIX diagnostics.

- 6. You will need the server firmware update file name in the next step. To view the name, enter the following at an AIX or Linux command prompt:

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

```
ls /tmp/fwupdate
```

The name of the server firmware update file is displayed. For example, you might see output similar to the following:

```
01SF2xx_yyy_zzz
```

- 7. To install the server firmware update, choose from the following options:
 - If you are updating AIX, enter the following at an AIX command prompt:


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

 where *fwlevel* is the specific server firmware update file name, such as 01SF2xx_yyy_zzz.
 - If you are updating Linux, enter the following at a Linux command prompt:


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

 where *fwlevel* is the specific server firmware update file name, such as 01SF2xx_yyy_zzz.

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

Note: If you receive a message stating: This partition does not have the authority to perform the requested function, see “Message regarding a server that was previously managed by an HMC” on page 201.

- 8. Continue with “Step 5. Verify that the update installed correctly” on page 165.

Related tasks

“Obtaining firmware updates through an HMC with an Internet connection” on page 141

Learn how to update or upgrade server firmware and power subsystem firmware (if you have a model 575 or 59x server) through an HMC when you have an Internet connection from the HMC or server.

“Obtaining firmware updates through an HMC using a CD, FTP server, or hard drive” on page 151

Learn how to update or upgrade server firmware and power subsystem firmware (if you have a model 575 or 59x server) through an HMC using a CD, FTP server, a hard drive to apply the update.

“Obtaining server firmware updates through IBM i5/OS” on page 166

Learn how to obtain server firmware updates through i5/OS.

“Working with the temporary and permanent side of the service processor” on page 208

Find out how to determine which side you are booting from, and how to switch to the other side if necessary.

“Using the AIX diagnostics to install the server firmware update through AIX” on page 204

Use this procedure if you want to use the AIX diagnostics to install the server firmware update through AIX to the temporary side of the service processor.

“Message regarding a server that was previously managed by an HMC” on page 201

Use this procedure to find out what to do if you receive a message regarding a server that was previously managed by an HMC.

Step 5. Verify that the update installed correctly:

1. Choose from the following options:

- To use the AIX or Linux command prompt (the operating system must be running and the diagnostics must be available), continue with the next step.
- To use the ASMI, view the level of server firmware displayed in the upper-right corner below the copyright statement on the ASMI Welcome pane; for example, SF220_006. If the level of server firmware displayed is not the level that you installed, refer to step 4.

2. Enter the following at a command prompt:

```
lsmcode
```

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

```
The current permanent system firmware image is SF220_005.
```

```
The current temporary system firmware image is SF220_006.
```

```
The system is currently booted from the temporary image.
```

Note:

- a. The permanent level is also known as the backup level.
 - b. The temporary level is also known as the installed level.
 - c. The system was booted from the temporary side, so at this time the temporary level is also the activated level.
3. Verify that the level of server firmware displayed is the level that you installed.
4. If the level of server firmware displayed is not the level that you installed, perform the following steps:
- a. Retry the update. If you created a CD or DVD for this procedure, use a new media.
 - b. If the problem persists, contact your next level of support.

Step 6. (Optional) Install the server firmware update 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 works correctly, you can permanently install the server firmware update.

Note: If you install the server firmware update 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 updates permanently, see “Installing a firmware update permanently” on page 170.

Related tasks

“Installing a firmware update permanently” on page 170
Find out how to permanently install a firmware update.

Obtaining server firmware updates through IBM i5/OS:

Learn how to obtain server firmware updates through i5/OS.

If you have i5/OS, you can download server firmware updates and operating system PTFs at the same time. If you have an HMC, you can either install the server firmware updates through the HMC, or install the server firmware and PTFs through i5/OS at the same time (except for the model 575 or 59x server). However, if there is a concurrent server firmware update available through the HMC, you might choose to use the HMC.

Important: Do not interrupt this process once you begin.

Note: Installing the server firmware updates through the operating system is a disruptive (nonconcurrent) process.

1. Do you have a model 575 or 59x server?
 - **No:** Continue with the next step.
 - **Yes:** You must use the HMC to install server firmware updates. Refer to one of the following procedures:
 - Obtaining server and power subsystem firmware updates through an HMC with an Internet connection.
 - Obtaining server firmware and power subsystem firmware updates through an HMC using a CD, FTP server, or hard drive.
2. Is your i5/OS server or logical partition managed by an HMC?
 - **No:** Continue with “Obtaining server firmware updates through i5/OS for a system not managed by an HMC.”
 - **Yes:** Continue with “Obtaining server firmware updates through IBM i5/OS for a system managed by an HMC” on page 167.

Related tasks

“Obtaining firmware updates through an HMC with an Internet connection” on page 141

Learn how to update or upgrade server firmware and power subsystem firmware (if you have a model 575 or 59x server) through an HMC when you have an Internet connection from the HMC or server.

“Obtaining firmware updates through an HMC using a CD, FTP server, or hard drive” on page 151

Learn how to update or upgrade server firmware and power subsystem firmware (if you have a model 575 or 59x server) through an HMC using a CD, FTP server, a hard drive to apply the update.

Obtaining server firmware updates through i5/OS for a system not managed by an HMC:

If you have i5/OS, you can download server firmware updates and operating system PTFs at the same time.

Important: Do not interrupt this process once you begin.

1. Is your i5/OS system or logical partition connected to the Internet?

- **Yes:** Continue with the next step.
 - **No:** You will need to order the update on CD. For details refer to Ordering fixes in the i5/OS Information Center. Once you have the CD, continue with the next step.
2. Use the i5/OS PTF installation functions on your service partition to install the server firmware updates.
 - For details on using updates, see Using software fixes in the i5/OS Information Center.
 - For instructions on how to install the server firmware updates along with i5/OS updates, see Installing fixes in the i5/OS Information Center.

Note: When you shut down the i5/OS service partition to install the server firmware updates, 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 updates are being installed. Allow the server to complete the processing; do not interrupt this process.

3. To verify that the fix installed correctly, refer to Verifying fix installation in the i5/OS Information Center.

For an overview of managing fixes, refer to Maintaining and managing i5/OS and related software in the i5/OS Information Center.

Obtaining server firmware updates through IBM i5/OS for a system managed by an HMC:

Your server is set up, by default, to download and install the server firmware updates using your HMC. Therefore, you need to change the default setting to enable your operating system to download and install the updates. In addition, you need to ensure that one of your logical partitions is designated to be a service partition. If your hardware is not connected to the Internet, you will also need to obtain a CD that contains the server firmware fix.

Important: Do not interrupt this process once you begin.

1. If you have more than one i5/OS logical partitions, designate one of your i5/OS logical partitions to be the service partition by following these steps:
 - a. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with the next step.
 - If you are using a an HMC with Version 7 or later, select **Managed system properties** in the General tab.
 - b. In the Navigation Area, open **Server and Partition**.
 - c. Select **Server Management**.
 - d. In the contents area, right-click the managed system and select **Properties**.
 - e. In the Service partition field, select the logical partition that you want to designate to be the service partition.
 - f. Click **OK**.
2. Prepare to change the update policy from the HMC to the i5/OS operating system.
 - a. Determine the level of server firmware that is on your managed system, and determine if any server firmware PTFs are installed on your service partition. For instructions on how to check the level of server firmware on the managed system and service partition, refer to the following:
 - If you are using Licensed Internal Code V5R4M0, see “Using IBM i5/OS to view the installed server firmware PTFs” on page 189.
 - If you are using Licensed Internal Code V5R4M5, see Displaying level of fixes in the i5/OS Information Center.
 - b. Choose from the following options:
 - If there *are* server firmware PTFs installed on the service partition, continue with step 2c on page 168.

- If there *are no* server firmware PTFs installed on the service partition, continue with step 3.
- c. Before changing your firmware update policy to i5/OS, ensure that the correct server firmware PTFs are installed on your service partition. The server firmware PTFs installed 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.

Important: When you set the firmware update policy to i5/OS, the current level of the server firmware PTFs installed on the service partition is used to update the server firmware that is running on the managed system. Consequently, if the server firmware PTFs installed on the service partition are 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.

3. Change the firmware update policy from the HMC to the i5/OS operating system using one of the following methods:
- **Advanced System Management Interface (ASMI):** To use the ASMI to change the firmware update policy from the HMC to the operating system, see *Changing firmware update policy*.

Note: You can access the ASMI through the HMC GUI, or point your browser to the ASMI. You will need the ASMI administrator login and password to access these menus.

- **HMC remote command line:** To change the firmware update policy using the HMC remote command line, specify the UPDLIC command.

Note: For more details on working 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:

```
updlc -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:

```
updlc -m xxxx -o h
```

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

4. If you are using Licensed Internal Code V5R4M5, enter the DSPFMWSTS (Display Firmware Status) command from the i5/OS service partition to automatically create the i5/OS server firmware product 57339xx in order to install server firmware PTFs.
5. Use the i5/OS PTF installation functions on your service partition to update the server firmware.
- For details on using updates, see *Using software fixes in the i5/OS Information Center*.
 - For instructions on how to order the server firmware updates along with the i5/OS updates, see *Ordering fixes in the i5/OS Information Center*.

When you shut down the i5/OS service partition to install the server firmware updates, 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 updates are being installed. Allow the server to complete the processing; do not interrupt this process.

6. To verify that the fix installed correctly, refer to *Verifying fix installation in the i5/OS Information Center*.

For an overview of managing fixes, see *Maintaining and managing i5/OS and related software in the i5/OS Information Center*.

Related information

Changing firmware update policy

Using the remote command line

Obtaining a specific firmware update with an HMC:

Find out how to download and install a specific level of server firmware or power subsystem firmware rather than the highest level of firmware.

You can download and install a specific level of firmware rather than the highest (most recent) level.

To get a specific firmware update, 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 firmware update, and click **OK**. For more information about each of the repositories, click **Help**.
8. In the Install and Activate (Implied Retrieve) window, choose from the following options:
 - If you want to get the highest level, click **OK**. Then continue with step 12.
 - If you want a specific level, select **Specific levels** for LIC level type, and click **OK**. Then continue with the next step.
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**.
10. 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.
11. Verify that the LIC type and LIC level displayed are correct, and click **OK**.
12. 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 firmware update now and activate the firmware update later, or select **Disruptive install and activate** if you want to install and activate the firmware level immediately, and click **OK**.
13. In the Hardware Management Console License Agreement window, read the agreement and click **Accept**.
14. In the Confirm the Action window, perform the required actions, and click **Finish**.

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

Perform the following steps:

- a. Use the usual procedures to shut down the logical partitions:
 - To shut down AIX logical partitions, see Shutting down AIX logical partitions.
 - To shut down i5/OS logical partitions, use the Power Down System (PWRDWN SYS RESTART *NO) command from an i5/OS command line (either in a 5250 emulator session on your HMC, or on the Operations Console). For further details, see Shutting down i5/OS logical partitions.
 - To shut down Linux logical partitions, see Shutting down Linux logical partitions.

- b. Power off the managed system.
- c. Restart the HMC after the server is off.
- d. Use the Change Licensed Internal Code Wizard to apply the firmware. Do not interrupt this process.
- e. Restart the managed system.
- f. Activate the Logical Partitions.

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

Installing a firmware update permanently:

Find out how to permanently install a firmware update.

After you download and install a firmware update, the update is temporarily installed until you install it permanently. 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 firmware update. Be aware that if you install the firmware update 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 firmware update 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 update. If you use i5/OS, you refer to this process as *applying* the update. If you use an HMC, you might refer to this process as *accepting* the update.

Using the HMC to install a firmware update permanently:

Find out how to use the HMC to permanently install a firmware update.

You might recognize the process of installing the firmware update 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 update. If you use i5/OS, you refer to this process as *applying* the update. If you use an HMC, you might refer to this process as *accepting* the update.

To permanently install the firmware update with an HMC, 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 firmware update.
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**.

Using AIX commands to install a firmware update permanently:

Find out how to use AIX commands to install a firmware update permanently.

You might recognize the process of installing the firmware update permanently by different terms, depending on the type of hardware or software you use. For example, for AIX or Linux, you might refer to this process as *committing* the update.

Note: To perform this task, you must meet the following criteria:

- You must have root user authority.
- You must start your server from the *temporary* side. For details, see Working with the temporary and permanent side of the service processor.

Use one of the following methods to install a firmware update permanently:

- Using the flash command
- Using the AIX diagnostic service aids

Using the flash command

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

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

The update_flash -c command might run for 10 or more minutes.
2. After the update completes, choose from the following options:
 - If you are committing a firmware update level that begins with SF220, use the manual process to shut down and restart the server. **This ends the procedure.**
 - If you are committing a firmware update level that begins with SF222 or higher, there is no need to shut down and restart the server. **This ends the procedure.**

Using the AIX diagnostic service aids

1. At the AIX command prompt, 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**. 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_006.
The system is currently booted from the temporary image.

Validate and Update System Firmware
Update System Firmware
Commit the Temporary Image
```
5. Select **Commit the Temporary Image**, and press Enter. The process might run for 10 or more minutes.
6. After the update is complete, choose from the following options:
 - If you are committing a firmware update level that begins with SF220, use the manual process to shut down and restart the server. **This ends the procedure.**
 - If you are committing a firmware update level that begins with SF222 or higher, there is no need to shut down and restart the server. **This ends the procedure.**

Related tasks

“Working with the temporary and permanent side of the service processor” on page 208

Find out how to determine which side you are booting from, and how to switch to the other side if necessary.

Using i5/OS to install a firmware update permanently:

Find out how to use i5/OS to install a firmware update permanently.

You might recognize the process of installing the firmware update permanently by different terms, depending on the type of hardware or software you use. For example, for i5/OS, you might refer to this process as *applying* the update. For more information, refer to Advanced fix installation: Applying fixes.

For i5/OS, you need to identify the PTFs that correspond to the server firmware update.

For details, see Advanced fix installation: Apply fixes.

Notes:

- If you are using Licensed Internal Code V5R4M0, the PTFs for server firmware updates are displayed with the Licensed Internal Code product (5722999) and begin with the prefix MH. For example, MHnnnnn, where nnnnn is the number associated to the specific server firmware update.
- If you are using Licensed Internal Code V5R4M5, use the Display Firmware Status (DSPFMWSTS) command to determine the i5/OS product and release for server firmware PTFs.

Using Linux commands to install a firmware update permanently:

Find out how to use Linux commands to install a firmware update permanently.

You might recognize the process of installing the firmware update permanently by different terms, depending on the type of hardware or software you use. For example, for AIX or Linux, you might refer to this process as *committing* the update.

Note: To perform this task, you must meet the following criteria:

- You must have root user authority.
 - You must start your server from the *temporary* side. For details, see Working with the temporary and permanent side of the service processor.
1. Ensure you have the following service tools installed on your server:
 - Platform Enablement Library – librtas-xxxxx.rpm
 - Service Aids – ppc64-utils-xxxxx.rpmwhere xxxxx represents a specific version of the RPM file.
 2. If you do not have the service tools on your server, refer to Obtaining service and productivity tools for Linux.
 3. After the service tools are installed to the server or partition running Linux, type the following at a Linux command prompt:
`/usr/sbin/update_flash -c`
The update_flash -c command might run for 10 or more minutes.
 4. Once the update completes, choose from the following options:
 - If you are committing a firmware update level that begins with SF220, use the manual process to shut down and restart the server. **This ends the procedure.**
 - If you are committing a firmware update level that begins with SF222 or higher, there is no need to shut down and restart the server. **This ends the procedure.**

Related tasks

“Working with the temporary and permanent side of the service processor” on page 208

Find out how to determine which side you are booting from, and how to switch to the other side if necessary.

“Obtaining service and productivity tools for Linux” on page 207

Find out about obtaining service and productivity tools for Linux.

Upgrading to a new firmware release through the HMC:

Find out how to upgrade to a new firmware release through the HMC.

The instructions for upgrading to a new firmware release through an HMC are included in the procedures for updating firmware through the HMC. For details, see the following:

- “Obtaining firmware updates through an HMC with an Internet connection” on page 141
- “Obtaining firmware updates through an HMC using a CD, FTP server, or hard drive” on page 151

Obtaining I/O adapter and device firmware updates

Learn how to apply I/O adapter and device firmware updates.

How you apply updates will depend on the type of update you are applying, whether you have an Internet connection from your HMC or server, and the operating system you are using.

Obtaining I/O adapter and device firmware updates through an HMC with an Internet connection (AIX only):

Learn how to obtain I/O adapter and device firmware updates with an HMC with an Internet connection.

The 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.

Related tasks

“Obtaining I/O adapter and device firmware updates for a system that is not managed by an HMC and is running AIX” on page 179

Learn how to obtain I/O adapter and device firmware updates for a system that is not managed by an HMC and is running AIX

Step 1. Ensure that you have an Internet connection:

To download updates from the service and support system or Web site to your HMC or server, you must have a connection to service and support either through a modem, direct or indirect Internet, or pass-through system.

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
 - a. In the navigation area, open **Service Applications**.
 - b. Select **Remote Support**.
 - c. Select **Customize Outbound Connectivity**.
 - d. Continue with step 4.
3. Perform the following steps:
 - a. In the Navigation area, click **Service Management**.
 - b. Select **Manage Outbound Connectivity**.
4. Select the tab for the type of outbound connectivity that you chose for your HMC (Local Modem, Internet VPN, or Pass-Through Systems). For more information about these settings, see Specifying the connection type from the HMC.

Note: If a connection to service and support does not exist, set up the service connection before proceeding with this procedure. For instructions on how to set up a connection to service and support, see Setting up your server to connect to service and support.

5. Click **Test**.
6. Verify that the test completes successfully. If the test is not successful, troubleshoot your connectivity and correct the problem before proceeding with this procedure. Alternatively, you can obtain the update on CD.

Step 2. Apply the I/O adapter and device firmware fix:

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2 on page 174.

- If you are using an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
 - a. From the HMC, expand the **Licensed Internal Code Maintenance** folder.
 - b. Click the **Licensed Internal Code Updates** icon.
 - c. In the Contents area, click **Change Licensed Internal Code**.
 - d. In the Target Object Selection window, click the target system, and click **OK**.
 - e. Continue with step 4.
 3. Perform the following steps:
 - a. In the Navigation area, click **Updates**.
 - b. Select the managed system.
 - c. In the Tasks area, click **Change Licensed Internal Code**.
 4. In the Change Licensed Internal Code window, select **Start Change Licensed Internal Code wizard**, and click **OK**.
 5. In the Specify LIC Repository window, choose from the following options:
 - If the HMC or server *is* connected to the Internet, select the repository location from which you want to download the fix, and click **OK**. The following options are available:
 - **IBM service Web site** (This site provides the most recent level of updates. You need a direct Internet connection to access this site.)
 - **IBM support system** (This site provides all available levels of updates. You can use a modem or direct Internet connection to access this site.)

For more information about each of the repository locations, click **Help**.
 6. In the Change Licensed Internal Code wizard welcome window, click **Next**.

Note: If there are no updates available, a message is displays that no updates 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 updates that are currently available to download and install from the selected repository:

- If server firmware updates or power subsystem firmware updates are available, the Change Licensed 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 updates or power subsystem updates now, click **Next**, and follow the instructions in the subsequent windows to install the firmware updates.

Notes:

- a. For all models except model 57x and 59x servers, install HMC updates before you install server firmware updates.
 - b. For model 57x and 59x servers, you *must* install HMC updates before you install server or power subsystem firmware updates. Then either install the server and power subsystem firmware updates together, or install the power subsystem and then the server firmware updates.
 - If you do not want to install the server firmware updates or power subsystem updates now, deselect **Managed System and Power LIC**, and click **Next**.
 - If I/O adapter and device firmware updates are available, the Change Licensed Internal Code wizard window is displayed, with **I/O LIC** either preselected or not selected.
7. In the Change Licensed Internal Code wizard window, ensure that **I/O LIC** is selected, and click **Advanced Options**.

8. In the Licensed Internal Code Survey Results window, select the adapters or devices for which you want to download and install firmware updates, and click **OK**.

Note: The system preselects the adapters or devices with the following characteristics:

- The HMC can manage the adapters or devices.
- Firmware updates are currently available.
- The adapters or devices do not need to be taken offline when you install the firmware updates.

You can change the preselected adapters or devices in the table to identify the I/O adapter and device firmware updates that you want to install.

Use the information in the Effect column 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 updates.

Use the information in the Suggested Action column 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. Refer to the procedure to obtain the updates through the operating system. For more information about the table, click **Help**.

9. In the Change Licensed Internal Code wizard window, click **Next**.
10. In the Hardware Management Console License Agreement window, read the agreement and click **Accept**.
11. In the Confirm the Action window, perform the required actions, and click **Finish**.
12. Continue with "Step 3. Verify that the fix installed correctly."

Step 3. Verify that the fix installed correctly:

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 4.
2. Ensure that the managed systems and power frames (if you have a model 575 or 59x server) are in the correct state.
 - a. From the HMC, select **Server and Partition**.
 - b. Select **Server Management** and ensure that the State is Power Off, Standby, or Operating.
 - c. If you have a model 575 or 59x server, select **Frame Management** and ensure that the state is Standby.
3. Perform the following steps:
 - a. From the HMC, expand the **Licensed Internal Code Maintenance** folder.
 - b. Click the **Licensed Internal Code Updates** icon.
 - c. Select **Change Licensed Internal Code for the current release**.
 - d. 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 firmware level.
 - e. In the Change Licensed Internal Code window, select **View system information**, and click **OK**.
 - f. Continue with 5.
4. Perform the following steps:
 - a. Click **Updates**.
 - b. Select the system.
 - c. In the Tasks area, click **View system information**.
5. In the Specify LIC Repository window, select **None**, and click **OK**. A window is displayed that shows system information for the target system.

6. In the window, click **View I/O Levels**.
7. In the Licensed Internal Code Survey Results window, verify that the firmware level indicated in the Current Level column matches the fix that you installed.
8. If the level of firmware displayed is not the level that you installed, you will need to apply it through the operating system. For details, refer to Obtaining I/O adapter and device firmware updates for a system that is not managed by an HMC and is running AIX.

Related tasks

“Obtaining I/O adapter and device firmware updates for a system that is not managed by an HMC and is running AIX” on page 179

Learn how to obtain I/O adapter and device firmware updates for a system that is not managed by an HMC and is running AIX

Obtaining I/O adapter and device firmware updates through an HMC using CD or an FTP server (AIX only):

Learn how to obtain I/O adapter and device firmware updates through an HMC when you want to use a CD or an FTP server to obtain the update (for AIX only).

The 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.

Related tasks

“Obtaining I/O adapter and device firmware updates for a system that is not managed by an HMC and is running AIX” on page 179


Learn how to obtain I/O adapter and device firmware updates for a system that is not managed by an HMC and is running AIX

Step 1. Download the I/O adapter and device firmware update:

You can download the update directly to your server, or you can download it to a computer with an Internet connection and create an update CD that you apply on the server. If necessary, contact service and support to order the update on CD.

Follow these step to download the I/O adapter and device update.

Note: To create a CD, you will need a CD burner and software. If you would prefer to order an update CD, contact service and support.

1. From a computer or server with an Internet connection, go to the Fix Central Web site at <http://www.ibm.com/eserver/support/fixes/> .
2. Select the appropriate family in the Product family list.
3. Select **Hardware microcode and firmware** in the Product list.
4. Click **Continue**.
5. Select your machine type and model from the drop-down list. An information window is displayed.
6. Click **Continue**. The available firmware levels are displayed.
7. Follow the on-screen prompts.
8. If you want to create a CD containing the update file, follow the instructions for your CD program.

Step 2. Apply the I/O adapter and device firmware update:

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 3 on page 177.
2. Perform the following steps:

- a. From the HMC, expand the **Licensed Internal Code Maintenance** folder.
- b. Click the **Licensed Internal Code Updates** icon.
- c. In the Contents area, click **Change Licensed Internal Code**.
- d. In the Target Object Selection window, click the target system, and click **OK**.
- e. Continue with step 4.
3. Perform the following steps:
 - a. In the Navigation area, click **Updates**.
 - b. Select the managed system.
 - c. In the Tasks area, click **Change Licensed Internal Code**.
4. In the Change Licensed Internal Code window, select **Start Change Licensed Internal Code wizard**, and click **OK**.
5. In the Specify LIC Repository window, choose from the following options:
 - If you have an update CD for this procedure, select **DVD drive** to install the update from CD, and click **OK**.
 - If you put the update on an FTP server, select **FTP site** and click **OK**.

For more information about each of the repository locations, click **Help**.
6. In the Change Licensed Internal Code wizard welcome window, click **Next**.

Note: If there are no updates available, a message is displays that no updates 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 updates that are currently available to download and install from the selected repository:

- If server firmware updates or power subsystem firmware updates are available, the Change Licensed 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 updates or power subsystem updates now, click **Next**, and follow the instructions in the subsequent windows to install the firmware updates.

Notes:

- a. For all models except model 57x and 59x servers, install HMC updates before you install server firmware updates.
- b. For model 57x and 59x servers, you *must* install HMC updates before you install server or power subsystem firmware updates. Then either install the server and power subsystem firmware updates together, or install the power subsystem and then the server firmware updates.
- If you do not want to install the server firmware updates or power subsystem updates now, deselect **Managed System and Power LIC**, and click **Next**.
- If I/O adapter and device firmware updates are available, the Change Licensed Internal Code wizard window is displayed, with **I/O LIC** either preselected or not selected.
7. In the Change Licensed Internal Code wizard window, ensure that **I/O LIC** is selected, and click **Advanced Options**.
8. In the Licensed Internal Code Survey Results window, select the adapters or devices for which you want to download and install firmware updates, and click **OK**.

Note: The system preselects the adapters or devices with the following characteristics:

- The HMC can manage the adapters or devices.
- Firmware updates are currently available.

- The adapters or devices do not need to be taken offline when you install the firmware updates.

You can change the preselected adapters or devices in the table to identify the I/O adapter and device firmware updates that you want to install.

Use the information in the Effect column 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 updates.

Use the information in the Suggested Action column 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. Refer to the procedure to obtain the updates through the operating system. For more information about the table, click **Help**.

9. In the Change Licensed Internal Code wizard window, click **Next**.
10. In the Hardware Management Console License Agreement window, read the agreement and click **Accept**.
11. In the Confirm the Action window, perform the required actions, and click **Finish**.
12. Continue with "Step 3. Verify that the update installed correctly."

Step 3. Verify that the update installed correctly:

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 4.
2. Ensure that the managed systems and power frames (if you have a model 575 or 59x server) are in the correct state.
 - a. From the HMC, select **Server and Partition**.
 - b. Select **Server Management** and ensure that the State is Power Off, Standby, or Operating.
 - c. If you have a model 575 or 59x server, select **Frame Management** and ensure that the state is Standby.
3. Perform the following steps:
 - a. From the HMC, expand the **Licensed Internal Code Maintenance** folder.
 - b. Click the **Licensed Internal Code Updates** icon.
 - c. In the Contents area, click **Change Licensed Internal Code**.
 - d. 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 firmware level.
 - e. In the Change Licensed Internal Code window, select **View system information**, and click **OK**.
 - f. Continue with step 5.
4. Perform the following steps:
 - a. Click **Updates**.
 - b. Select the system.
 - c. In the Tasks area, click **View system information**.
5. In the Specify LIC Repository window, select **None**, and click **OK**. A window is displayed that shows system information for the target system.
6. In the window, click **View I/O Levels**.
7. In the Licensed Internal Code Survey Results window, verify that the firmware level indicated in the Current Level column matches the fix that you installed.
8. If the level of firmware displayed is not the level that you installed, you will need to apply it through the operating system. For details, refer to Obtaining I/O adapter and device firmware updates for a system that is not managed by an HMC and is running AIX.

Related tasks

“Obtaining I/O adapter and device firmware updates for a system that is not managed by an HMC and is running AIX”


Learn how to obtain I/O adapter and device firmware updates for a system that is not managed by an HMC and is running AIX

Obtaining I/O adapter and device firmware updates for a system that is not managed by an HMC and is running AIX:

Learn how to obtain I/O adapter and device firmware updates for a system that is not managed by an HMC and is running AIX

The 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.

If you do not use an HMC to manage your server, you must obtain your updates through your operating system. In this situation, you can obtain I/O adapter and device firmware updates using the AIX commands.

1. Do you have AIX and use an HMC, or an IBM eServer p5 or System p5 that is managed by an HMC?
 - **No:** Continue with the next step.
 - **Yes:** You will need to apply I/O adapter and device firmware updates through the HMC. Refer to one of the following procedures depending on whether you have an Internet connection:
 - Obtaining I/O adapter and device firmware updates through an HMC with an Internet connection (AIX only)
 - Obtaining I/O adapter and device firmware updates through an HMC using CD or an FTP server (AIX only)
2. From a computer or server with an Internet connection, go to the Fix Central Web site at <http://www.ibm.com/eserver/support/fixes/> .
3. Select the appropriate family in the Product family list.
4. Select **Hardware microcode and firmware** in the Product list.
5. Click **Continue**.
6. Perform the following steps:
 - a. Select your machine type and model from the drop-down list. An information window is displayed.
 - b. Click **Continue**. The available firmware levels are displayed.
 - c. Follow the on-screen instructions to download and install the I/O adapter and device firmware update to your system.

Related tasks

“Obtaining I/O adapter and device firmware updates through an HMC with an Internet connection (AIX only)” on page 173

Learn how to obtain I/O adapter and device firmware updates with an HMC with an Internet connection.

“Obtaining I/O adapter and device firmware updates through an HMC using CD or an FTP server (AIX only)” on page 176

Learn how to obtain I/O adapter and device firmware updates through an HMC when you want to use a CD or an FTP server to obtain the update (for AIX only).

Obtaining I/O adapter and device firmware updates through IBM i5/OS:

Learn how to obtain I/O adapter and device firmware updates through i5/OS.

The 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.

For i5/OS, I/O adapter and device firmware PTFs for i5/OS systems and logical 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 updates. For instructions on how to install i5/OS updates, refer to Order fixes in the i5/OS Information Center.


Obtaining operating system updates

Learn how to download and install updates for your operating systems.

Obtaining operating system updates for AIX or Linux:

Learn how to download and install updates for your operating systems.

To keep your operating system or logical partitions running smoothly, it is important that you install updates for your operating system code when they are available.

1. Go to the Fix Central Web site at <http://www.ibm.com/eserver/support/fixes/> .
2. Select the appropriate family in the Product family list. For example, UNIX servers.
3. In the Product list, click the operating system for which you want to get a update.
4. Depending on your selections, you might see additional lists from which you can select specific options.
5. Click **Continue**.

For more information about updates for the operating systems, see the Support for IBM System p Web site at


<http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/brandmain?brandind=5000025>



Obtaining operating system updates for i5/OS:

Learn how to download and install updates for your operating systems.

To keep your operating system or logical partitions running smoothly, it is important that you install updates for your operating system code when they are available.

1. Go to the Fix Central Web site at <http://www.ibm.com/eserver/support/fixes/> .
2. Select the appropriate family in the Product family list. For example, **System i family**.
3. In the Product list, click the operating system for which you want to get an update.
4. Depending on your selections, you might see additional lists from which you can select specific options.
5. Click **Continue**.

For more information about updates for the operating systems, refer to Maintaining and managing i5/OS and related software in the i5/OS Information Center.

Obtaining updates for the Virtual I/O Server

Learn about obtaining updates to the firmware on the Virtual I/O Server, and for the firmware on the devices that the Virtual I/O Server manages.

You can update the Virtual I/O Server's firmware and device microcode through the Integrated Virtualization Manager or by using the command line interface.

If you do not have an Internet connection from the system, you will need to obtain the update on CD.

You can use the information on the Virtual I/O Server update Web site to download and install the latest fix packs and updates on the management partition of the managed system. For more information about the methods that you can use to install these updates, see the Virtual I/O Server update Web site.

Related information

 [Virtual I/O Server update Web site](#)

Updating the Virtual I/O Server's firmware and device microcode through the Integrated Virtualization Manager with an Internet connection:

Learn how to use the Integrated Virtualization Manager (IVM) to generate a microcode survey of the managed system and to download and upgrade microcode when you have an Internet connection from your system.

Perform Step 1 through 3 to update the Virtual I/O Server's firmware and device microcode through the IVM when you have an Internet connection from the management partition.

Note: Updating server firmware is a disruptive process.

Step 1. View the existing firmware level:

1. Under the **Service Management** menu, click **Updates**. The Updates page is displayed.
2. Select the **Microcode Updates** tab.
3. Click **Generate New Survey**. A list of devices is displayed.
4. Record the current level of firmware that is displayed for *Type: system*.

Step 2. Apply firmware and device microcode using the IVM:

1. Note the following:
 - If you update the server firmware for device sys0, you will need to shut down all client logical partitions before applying the firmware.
 - If you update some device's microcode, you might need to take the device offline using the `rmdev` command before applying the firmware.
2. Under the **Service Management** menu, click **Updates**. The Updates page is displayed, which contains the Management Partition Updates tab and the Microcode Updates tab.
3. Select the **Microcode Updates** tab.
4. The Microcode download base path field should default to the correct address. Do not change it.
5. Click **Generate New Survey**. A list of devices is displayed.
6. From the Microcode Survey Results list, select one or more items to upgrade.

Note: If you select to update the firmware for device sys0, the system will shut down and restart when you apply the firmware. If you select a device, you might need to take the device offline. You can view the Impact column to determine the action you need to take. You will want to perform the action before you issue the command to install the update in step 13 on page 182.

7. Click the **Download** link in the task area. Information about the selected devices, such as the available microcode level and the commands you need in order to install the microcode updates, is displayed.
8. Record the commands, you will need them later in the procedure.

Tip: You might want to copy and paste the commands you need to a text document.

9. Select the **Accept license** check box in the work area.
10. Click **OK** to download the selected microcode and store it on the disk.
11. Telnet IVM using a terminal emulator, for example, IBM Personal Communications for Windows®.
12. Log into the IVM.
13. Issue the appropriate command to install the update that you recorded in step 8 on page 181.

Note: If you copied the commands to a text document, you can paste them in.

Step 3. Verify that the firmware updated correctly:

If you prefer to use the command line, refer to Lsfware Command.

1. Under the **Service Management** menu, click **Updates**. The Updates page is displayed, which contains the Management Partition Updates tab and the Microcode Updates tab.
2. Select the **Microcode Updates** tab.
3. Click **Generate New Survey**. A list of devices is displayed.
4. Ensure that the current level of firmware that is displayed for *Type: system* matches the level you installed.

Related information

Lsfware Command

Updating the Virtual I/O Server's firmware and device microcode through the Integrated Virtualization Manager without an Internet connection:

Learn how to use the Integrated Virtualization Manager (IVM) to update the Virtual I/O Server's firmware and device microcode when you do not have an Internet connection from the managed system.


Perform steps 1 through 4 to update the Virtual I/O Server's firmware and device microcode through the IVM when you do not have an Internet connection from the management partition.

Step 1. View the existing firmware level:

1. Under the **Service Management** menu, click **Updates**. The Updates page is displayed.
2. Select the **Microcode Updates** tab.
3. Click **Generate New Survey**. A list of devices is displayed.
4. Record the current level of firmware that is displayed for *Type: system*.

Step 2. View or download the firmware fix:

Follow this procedure to view or download the firmware update. You can download the update directly to your server, or you can download it to a computer with an Internet connection and create an update CD that you apply on the server. If necessary, contact service and support to order the update on CD.

1. From a computer or server with an Internet connection, go to the Fix Central Web site at <http://www.ibm.com/eserver/support/fixes/> .
2. Select the appropriate family in the Product family list.
3. Select **Hardware microcode and firmware** in the Product list.
4. Click **Continue**.
5. From the Microcode downloads Web site, perform the following steps:
 - a. Select your machine type and model from the drop-down list. An information window is displayed.
 - b. Click **Continue**.
 - c. Click **Desc**. An HTML file is displayed.

- d. In the Description file, click the .ISO file. For example, SF2aa_bbb_BP2cc_ddd.iso.

Note: If the ISO image is unavailable, you will need to order it. For details, contact service and support.

- e. Follow the on-screen prompts.
- f. Follow the instructions for your CD program to create a CD from the ISO image. Then go to “Step 3. Apply firmware and device microcode using the IVM.”

Step 3. Apply firmware and device microcode using the IVM:

1. Note the following:
 - If you update the server firmware for device sys0, you will need to shut down all client logical partitions before applying the firmware.
 - If you update some device’s microcode, you might need to take the device offline using the `rmdev` command before applying the firmware.
2. Insert the CD into the CD drive for the managed system.
3. Under the **Service Management** menu, click **Updates**. The Updates page is displayed, which contains the Management Partition Updates tab and the Microcode Updates tab.
4. Select the **Microcode Updates** tab.
5. In the Microcode download base path field, type `optical_device_path/microcode/` (for example, `/dev/cd0/microcode/`).

Note: Ensure you type `/microcode/` after the optical device path, or the firmware will not be found.

6. Click **Generate New Survey**. A list of devices is displayed.
7. From the Microcode Survey Results list, select one or more items to upgrade.

Note: If you select to update the firmware for device sys0, the system will shut down and restart when you apply the firmware. If you select a device, you might need to take the device offline. You can view the Impact column to determine the action you need to take. You will want to perform the action before you issue the install command in step 14.

8. Click the **Download** link in the task area. Information about the selected devices, such as the available microcode level and the commands you need in order to install the microcode updates, is displayed.
9. Record the commands, you will need them later in the procedure.

Tip: You might want to copy and paste the commands you need to a text document.

10. Select the **Accept license** check box in the work area.
11. Click **OK** to download the selected microcode and store it on the disk.
12. Telnet IVM using a terminal emulator, for example, IBM Personal Communications for Windows.
13. Log into the IVM.
14. Issue the appropriate install command that you recorded in step 9.

Note: If you copied the commands to a text document, you can paste them in.

Step 4. Verify that the firmware updated correctly:

If you prefer to use the command line, refer to Lsfware Command.

1. Under the **Service Management** menu, click **Updates**. The Updates page is displayed, which contains the Management Partition Updates tab and the Microcode Updates tab.
2. Select the **Microcode Updates** tab.
3. Click **Generate New Survey**. A list of devices is displayed.

4. Ensure that the current level of firmware that is displayed for *Type: system* matches the level you installed.

Related information

Lsfware Command

Updating the Virtual I/O Server's firmware using the command line interface:

Learn about using the command line interface to apply updates to the firmware on your Virtual I/O Server.

To obtain updates to the management partition or to obtain microcode updates using the command line interface, refer to Updating the Virtual I/O Server using the command-line interface.

Related information

Updating the Virtual I/O Server using the command-line interface

Updating the firmware of the devices that the Virtual I/O Server manages:

Learn how to update the firmware of the devices that the Virtual I/O Server manages.

To update the firmware for devices managed by the Virtual I/O Server or Integrated Virtualization Manager, choose from the following options:

- To update the device's firmware using the Integrated Virtualization Manager, see Obtaining updates for the Virtual I/O Server.
- To update the device's firmware using the command-line interface, refer to the following command descriptions:
 - invscout
 - Lsfware Command
 - Ldfware Command

Related tasks

"Obtaining updates for the Virtual I/O Server" on page 140

Learn about obtaining updates to the firmware on the Virtual I/O Server, and for the firmware on the devices that the Virtual I/O Server manages.

Related information

invscout

Lsfware

Ldfware

Obtaining updates for a clustered environment

Learn how to obtain updates for the clustered server.

There are several types of updates you might need to apply when you use a clustered environment. The updates include server firmware, HMC if you have one, and I/O adapter and devices.

Choose the type of updates you want to apply:

- "Obtaining HMC machine code updates and upgrades" on page 121
- "Obtaining firmware updates" on page 135
- "Obtaining I/O adapter and device firmware updates" on page 173
- "Obtaining operating system updates" on page 180

Managing updates

Learn about tasks you can perform to manage updates.

Ensuring you have a connection to service and support

Find out how to ensure that you have a connection to service and support.

To download updates from the service and support system or Web site to your HMC or server, you must have a connection to service and support either through a modem, direct or indirect Internet, or pass-through system.

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
 - a. In the navigation area, open **Service Applications**.
 - b. Select **Remote Support**.
 - c. Select **Customize Outbound Connectivity**.
 - d. Continue with step 4.
3. Perform the following steps:
 - a. In the Navigation area, click **Service Management**.
 - b. Select **Manage Outbound Connectivity**.
4. Select the tab for the type of outbound connectivity that you chose for your HMC (Local Modem, Internet VPN, or Pass-Through Systems). For more information about these settings, see Specifying the connection type from the HMC.

Note: If a connection to service and support does not exist, set up the service connection before proceeding with this procedure. For instructions on how to set up a connection to service and support, see Setting up your server to connect to service and support.

5. Click **Test**.
6. Verify that the test completes successfully. If the test is not successful, troubleshoot your connectivity and correct the problem before proceeding with this procedure. Alternatively, you can obtain the update on CD.

Determining your HMC machine code version and release

Find out how to view the HMC machine code version and release.

The level of machine code on the HMC will determine the available features, including concurrent server firmware maintenance and enhancements to upgrading to a new release.

1. Choose from the following options:
 - If you are using an HMC Version 6 or earlier, continue with step 2.
 - If you are using an HMC Version 7 or later, continue with step 7.
2. In the navigation area, open **Licensed Internal Code Maintenance**.
3. Select **HMC Code Update**.
4. In the contents area, look for the version and release of your HMC machine code in the Status area.
5. Record the version and release.
6. If you need to update your HMC machine code version and release, see Obtaining HMC machine code updates and upgrades. **This ends the procedure.**
7. In the Navigation area, click **Updates**.
8. In the Work area, view and record the information that appears under the HMC Code Level heading, including: the HMC version, release, maintenance level, build level, and base versions.
9. If you need to update your HMC machine code version and release, see Obtaining HMC machine code updates and upgrades. **This ends the procedure.**

Related concepts

“Obtaining HMC machine code updates and upgrades” on page 121
Learn how to obtain HMC machine code updates and upgrades.

Viewing existing firmware levels

Find out how to view the level of firmware that currently runs on your server.

You can view the current and backup levels of server and power subsystem firmware on the managed system.

Using the HMC to view the existing firmware levels:

Learn how to view the level of firmware that currently runs on your server using the HMC.

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 4.
2. Ensure that the managed systems and power frames (if you have a model 575 or 59x server) are in the correct state.
 - a. From the HMC, select **Server and Partition**.
 - b. Select **Server Management** and ensure that the State is Power Off, Standby, or Operating.
 - c. If you have a model 575 or 59x server, select **Frame Management** and ensure that the state is Standby.
3. Perform the following steps:
 - a. In the navigation area, open **Licensed Internal Code Maintenance** folder.
 - b. Click the **Licensed Internal Code Updates** icon.
 - c. Select **Change Licensed Internal Code for the current release**.
 - d. 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 firmware level.
 - e. In the Change Licensed Internal Code window, select **View system information**, and click **OK**.
 - f. 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 firmware that has been installed and will be installed into memory after the managed system is powered off and powered on.
 - The *Activated Level* indicates the level of firmware that is active and running in memory.
 - The *Accepted Level* indicates the backup level of firmware. You can return to the backup level of firmware if you decide to remove the installed level.
 - g. Record the installed level and click **Close**.
 - h. Click **Cancel**.
4. In the Navigation area, click **Updates**.
5. Ensure that the managed system Status is Power Off, Standby, or Operating.
6. Record the level that appears in the EC Number field. For example, 01EM310.

Using the ASMI to view the existing level of server firmware:

Find out how to use the ASMI to view the level of firmware that currently runs on your server.

On the ASMI Welcome pane, view the existing level of server firmware in the upper-right corner below the copyright statement, for example, SF220_006.

Using the AIX or Linux command line to view the existing firmware level:

Learn how to view the current firmware level using the AIX or Linux command line.

You must have AIX diagnostics installed on your server to perform this task

1. Choose from the following options:

- To use the AIX command line, continue with the next step.
- To use the Linux command line, continue with step 3.
- To use the AIX or Linux command line when you are using a 7037-A50 or 7047-185 system, continue with step 5.

2. At an AIX command prompt, enter the following command:

```
lsmcode
```

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

The current permanent system firmware image is SF220_005.

The current temporary system firmware image is SF220_006.

The system is currently booted from the temporary image.

Note:

- a. The permanent level is also known as the backup level.
- b. The temporary level is also known as the installed level.
- c. The system was booted from the temporary side, so at this time the temporary level is also the activated level.

3. To view existing levels of server firmware for Linux, you must have the following service tools installed on 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.

Note: If you do not have the service tools on your server, refer to “Obtaining service and productivity tools for Linux” on page 207.

4. After the service tools are installed on the server running Linux, enter the following at a Linux command prompt:

```
lsmcode
```

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

Version of system firmware is: 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.	The backup level.	The activated level.
Also known as the temporary level.	Also known as the permanent level.	The level on which the server is currently running.

5. If you have a 7037-A50 or 7047-185 system, choose from the following options:

- If are using AIX, continue with the next step.
- If you are using Linux, continue with step 7 on page 188.

6. At an AIX command line, enter the following command:

```
lsmcode
```

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

The current permanent system firmware image is AT061_055.

The current temporary system firmware image is AT061_058.

The system is currently booted from the temporary image.

Note: When the lsmcode command is run on a 7037-A50 or 7047-185 system, the temporary or permanent side of the flash might report `_UNKNOWN_` for the firmware level. This occurs because there is only one level of base motherboard controller firmware. The level is `_UNKNOWN_` when it is not included with the system firmware.

When you install new firmware, it is installed onto the temporary side by default. This new firmware level includes a new level of base motherboard controller code, and will cause `_UNKNOWN_` to be reported for the permanent side. This is not a problem; it indicates that the firmware levels in the flash are not a combination that is included from the factory.

To update the firmware so that `_UNKNOWN_` is not reported, perform the following steps:

- a. Perform a commit operation using the appropriate operating system command.
 - b. After the commit operation is complete, restart the system.
 - c. When the system has restarted and the operating system is running, rerun the lsmcode command. Both the T and P should report a level (such as AT206_061) instead of `_UNKNOWN_`.
7. To view existing levels of server firmware for Linux, you must have the following service tools installed on 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.

Note: If you do not have the service tools on your server, refer to “Obtaining service and productivity tools for Linux” on page 207.

8. After the service tools are installed to the server running Linux, enter the following at a Linux command line:

```
lsmcode
```

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

```
Version of system firmware is: AT061_058(t) AT061_055(p) AT061_058(t)
```

Note: When the lsmcode command is run on a 7037-A50 or 7047-185 system, the temporary or permanent side of the flash might report `_UNKNOWN_` for the firmware level. This occurs because there is only one level of base motherboard controller firmware. The level is `_UNKNOWN_` when it is not included with the system firmware.

When you install new firmware, it is installed onto the temporary side by default. This new firmware level includes a new level of base motherboard controller code, and will cause `_UNKNOWN_` to be reported for the permanent side. This is not a problem; it indicates that the firmware levels in the flash are not a combination that is included from the factory.

To update the firmware so that `_UNKNOWN_` is not reported, perform the following steps:

- a. Perform a commit operation using the appropriate operating system command.

- b. After the commit operation is complete, restart the system.
- c. When the system has restarted and the operating system is running, rerun the lsmcode command.
Both the T and P should report a level (such as AT206_061) instead of _UNKNOWN_.

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

Server firmware levels displayed		
AT061_058 (t)	AT061_055 (p)	AT061_058 (t)
The temporary level.	The permanent level.	The level on which the server is currently running.

Related tasks

“Obtaining service and productivity tools for Linux” on page 207
Find out about obtaining service and productivity tools for Linux.

Using IBM i5/OS to view the installed server firmware PTFs:

There are several methods you can use to view the installed server firmware PTFs on your system.

1. Choose from the following options:
 - If you are using Licensed Internal Code V5R4M0, continue with the next step.
 - If you are using Licensed Internal Code V5R4M5, see Displaying level of fixes in the i5/OS Information Center.
2. Type STRSST at an i5/OS command line and press Enter. The Start Service Tools (SST) Sign On display is displayed.
3. Type in your user ID and password and press Enter.
4. Select Start a Service Tool.
5. Select Display/Alter/Dump.
6. Select Display/Alter storage.
7. Select Licensed Internal Code (LIC) data.
8. Scroll down and select Advanced analysis.
9. Scroll down and select FLASHLEVELS.
10. When the Specify Advanced Analysis Options screen is displayed, press Enter.

Following is an example of what might be displayed:

```
DISPLAY/ALTER/DUMP
Running macro: FLASHLEVELS
```

```
LS Flash Sync Enabled.
HMC MANAGED
Base Level:
```

Side	Date/Time	MI Keyword	PTFs
-----	-----	-----	-----
Memory	20060616/1703	SFxxx_xxx	MH00xxx
Flash P	20060607/1258	SFxxx_xxx	MH00xxx
Flash T	20060616/1703	SFxxx_xxx	MH00xxx
Load Source A	20060507/1345	SFxxx_xxx	MH00xxx
Load Source B	20060607/1258	SFxxx_xxx	MH00xxx

The PTFs for server firmware updates are displayed with the Licensed Internal Code product (5722999) and begin with the prefix MH. For example, MHnnnnn where nnnnn is the number associated to the specific server firmware fix.

11. If the level of server firmware displayed is not the level that you installed, perform the following steps:
 - a. Retry the update. If you created a CD or DVD for this procedure, use a new media.
 - b. If the problem persists, contact your next level of support.

Viewing available firmware levels

Find out how to view the levels of firmware that are available for you to download as fixes.

Viewing available firmware levels with an HMC (with an Internet connection):

Find out how to view the levels of firmware that are available for you to download as fixes.

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
 - a. From the HMC, expand the **Licensed Internal Code Maintenance** folder.
 - b. Click the **Licensed Internal Code Updates** icon.
 - c. In the Contents area, click **Change Internal Code for the current release**.
 - d. In the Target Object Selection window, click the target system, and click **OK**.
 - e. In the Change Internal Code window, select **View system information**.
 - f. Continue with step 4.
3. Perform the following steps:
 - a. In the Navigation area, click **Updates**.
 - b. Select the target system.
 - c. In the Task area, select **View system information**.
4. In the Specify LIC Repository window, select the repository location from which you want to view available firmware updates, and click **OK**. The following options are available:
 - **IBM service Web site** (This site provides the most recent level of updates. You need a direct Internet connection to access this site.)
 - **IBM support system** (This site provides all available levels of updates. You can use a modem or direct Internet connection to access this site.)
 - **DVD-RAM media:** Select this option if you previously put the update on CD and it is in the DVD drive on the HMC.

Note: If you choose the DVD-RAM media repository and receive an I/O error when using a CD that you created, it might mean that the software you used to create the CD does not conform to the requirements for writing of temporary records on the HMC.

- **FTP site:** Select this option if you previously downloaded the update to an FTP site. (This site would be setup previously by your organization's advanced support personnel.) An FTP server is any system on which the FTP server protocol is activated. If you select the FTP site, you need to know the following information:

Note: Usually, a PC has only the FTP client active.

- **FTP site** - The fully qualified host and domain name of the FTP server from which you want to download the update.
- **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 or power subsystem firmware update. You can specify the default directory `/opt/ccfw/data` if you placed the update in that directory, or you can change the directory path if the update is in a directory other than the

default directory. For example, if you downloaded the update and copied it to a unique directory on the FTP server, you can specify that directory.

- **Hard drive:** Select this option if you previously downloaded the update to the hard disk drive on your HMC. (This repository can be selected after a successful Code Update for this release was the last completed update to another Managed System or Power Subsystem by this HMC.)

Note: For more information about each of the repository locations, click **Help**.


A window is displayed that shows system information for the target system, including the retrievable levels of firmware. For details on retrievable levels of firmware, see *Levels of firmware (Licensed Internal Code)* on the HMC.

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

5. Record the available firmware level or levels.

Viewing available firmware levels for AIX and Linux:


Find out how to view the levels of firmware that are available for you to download.

1. From a computer or server with an Internet connection, go to the Fix Central Web site at <http://www.ibm.com/eserver/support/fixes/> 
2. Select the appropriate family in the Product family list.
3. To view available levels for AIX or Linux, perform the following steps:
 - a. Select **Hardware microcode and firmware** in the Product or fix type list.
 - b. Click **Continue**.
4. Perform the following steps:
 - a. Select your machine type and model from the drop-down list. An information window is displayed.
 - b. Click **Continue**. The available firmware is displayed.
 - c. View and record the available server firmware and power subsystem firmware (if you have a model 575 or 59x server). For more details, click **Desc**.

Viewing available firmware levels for IBM i5/OS:

Find out how to view the levels of firmware that are available for you to download as fixes.

To view available firmware for i5/OS, follow these steps:

1. From a computer or server with an Internet connection, go to the Fix Central Web site at <http://www.ibm.com/eserver/support/fixes/> .
2. In the Server field select **iSeries family**.
3. In the Product or fix type field select **Server firmware**.

Note: This selection includes both server firmware and power subsystem firmware (if you have a model 575 or 59x server).

4. In the Firmware update policy field, select **Update policy set to HMC**.
5. Click **Continue**.
6. In the Server firmware fixes window, click **Recommended fixes**.
7. From the Recommended fixes page, select your version and release in the Select your release field (for example, V5R4).
8. Select **Server Firmware: Update Policy Set to HMC** from the select a topic list.

9. Click **Go**.
10. Record the available levels that are displayed.

Notes:

- If you are using Licensed Internal Code V5R4M0, the PTFs for server firmware are displayed with the Licensed Internal Code product (5722999) and begin with the prefix MH. For example, MHnnnnn where nnnnn is the number associated to the specific server firmware fix.
- If you are using Licensed Internal Code V5R4M5, use the Display Firmware Status (DSPFMWSTS) command to determine the i5/OS product and release for server firmware PTFs.

Determining if your server firmware level and HMC machine code level are compatible

Learn how to find out if your server firmware level and HMC machine code level are compatible.

The HMC machine code needs to be equal to or greater than the server firmware level. Also, if an HMC manages multiple servers at different firmware release levels, the HMC machine code level must be equal to or higher than the system firmware level on the server that is at the latest release level. During this procedure you will find out how to ensure your HMC machine code and server firmware is compatible.

You *must* install HMC updates before you install server firmware or power subsystem firmware updates so that the HMC can handle any updates or new function that you apply to the server. After you install HMC updates, either install the power subsystem firmware and server firmware updates together, or install the power subsystem firmware first (if you have a model 575 or 59x server), and then the server firmware second.

Step 1. Review your HMC machine code version and release:

The level of HMC machine code that you have will determine the available features, including concurrent server firmware maintenance and enhancements to upgrading to a new release.

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 3.
2. Perform the following steps:
 - a. In the navigation area, open **Licensed Internal Code Maintenance**.
 - b. Select **HMC Code Update**.
 - c. In the contents area, look for the version and release of your HMC machine code in the Status area.
 - d. Record the version and release.
 - e. Continue with "Step 2. View existing firmware levels with an HMC."
3. Perform the following steps:
 - a. In the Navigation area, click **Updates**.
 - b. In the Work area, view and record the information that appears under the HMC Code Level heading, including: the HMC version, release, maintenance level, build level, and base versions.
 - c. Continue with "Step 2. View existing firmware levels with an HMC."

Step 2. View existing firmware levels with an HMC:

1. Choose from the following options:
 - If you are using an HMC with Version 6 or earlier, continue with step 2.
 - If you are using an HMC with Version 7 or later, continue with step 4 on page 193.
2. Ensure that the managed systems and power frames (if you have a model 575 or 59x server) are in the correct state.

- a. From the HMC, select **Server and Partition**.
 - b. Select **Server Management** and ensure that the State is Power Off, Standby, or Operating.
 - c. If you have a model 575 or 59x server, select **Frame Management** and ensure that the state is Standby.
3. Perform the following steps:
 - a. From the HMC, expand the **Licensed Internal Code Maintenance** folder.
 - b. Click the **Licensed Internal Code Updates** icon.
 - c. Select **Change Licensed Internal Code for the current release**.
 - d. 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 firmware level.
 - e. In the Change Licensed Internal Code window, select **View system information**, and click **OK**.
 - f. 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 firmware that has been installed and will be installed into memory after the managed system is powered off and powered on.
 - The *Activated Level* indicates the level of firmware that is active and running in memory.
 - The *Accepted Level* indicates the backup level of firmware. You can return to the backup level of firmware if you decide to remove the installed level.
 - g. Record the installed level and click **Close**.
 - h. Click **Cancel**.
 - i. For information on compatible levels of HMC machine code and system firmware, refer to the POWER code matrix Web site.
 4. Perform the following steps:
 - a. In the Navigation area, click **Updates**.
 - b. Ensure that the managed system Status is Power Off, Standby, or Operating.
 - c. Record the level that appears in the EC Number field. For example, 01EM310.
 - d. For information on compatible levels of HMC machine code and system firmware, refer to the POWER code matrix Web site.

Related information

 [POWER5 Code Matrix Web site](#)

Step 3. Update HMC machine code or server firmware:

Choose from the following options:

- If you need to update the HMC machine code, see “Obtaining HMC machine code updates and upgrades” on page 121.
- If you need to apply a later version of server firmware, see Obtaining firmware updates.
- If you have a model 570 or 9116-561, and after exchanging the service processor assembly you need to apply an earlier level of server firmware for certification requirements, refer to Using an HMC to apply an earlier level of server firmware after exchanging the service processor in a model 570 or 9116-561.

Important: Only apply an earlier level of server firmware if it is a certification requirement.

Related concepts

“Obtaining HMC machine code updates and upgrades” on page 121

Learn how to obtain HMC machine code updates and upgrades.

“Obtaining firmware updates” on page 135

Learn how to obtain firmware updates.

Related tasks

“Using an HMC to apply an earlier level of server firmware after exchanging the service processor in a model 570 or 9116-561” on page 198

Learn how to use the HMC to apply an earlier level of server firmware if it is a certification requirement.

Viewing the firmware history or cover letter

Find out how to view the firmware history or cover letter.

Server and power subsystem firmware updates can correct known problems or add new function to the code in your current firmware release. To find out what problems the firmware update will correct, or to find out what new function is included in the firmware update, you can view the firmware history or cover letter.

Viewing the firmware cover letter with an HMC:

Find out how to view the firmware cover letter with an HMC.

To view the firmware 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**.
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 firmware fix cover letter, and click **View Details**.
For example, you might select **Managed System**. The firmware fix cover letter is displayed.
11. Read the cover letter to learn about what problems the firmware fix will correct, or to find out what new function is included in the firmware fix.

Viewing the firmware history for AIX or Linux:

Find out how to view the firmware history information for AIX or Linux.

You can view firmware history in several places. For example, you can view history information from the Fix Central Web site, or you can read the history information that accompanies the fix CDs.

To view the firmware history from the Fix Central Web site, follow these steps:

1. From a computer or server with an Internet connection, go to the Fix Central Web site at <http://www.ibm.com/eserver/support/fixes/> .
2. Select the appropriate family in the Product family list.
3. Select **Hardware microcode and firmware** in the Product list.
4. Click **Continue**.
5. Perform the following steps:
 - a. Select your machine type and model from the list. An information window is displayed.
 - b. Click **Continue**. The available firmware levels are displayed.
 - c. Click **Desc**. An HTML document is displayed.
 - d. Review the information that is displayed to learn more about what is included in the firmware update.

Viewing the firmware cover letter for IBM i5/OS:

There are several methods you can use to view the firmware cover letter.

To view the server firmware fix cover letter, you need to identify the PTFs that correspond to the server firmware fixes. For details, refer to Working with fix cover letters in the i5/OS Information Center.

Notes:


- If you are using Licensed Internal Code V5R4M0, the PTFs for server firmware are displayed with the Licensed Internal Code product (5722999) and begin with the prefix MH. For example, *MHnnnnn* where *nnnnn* is the number associated to the specific server firmware fix.
- If you are using Licensed Internal Code V5R4M5, use the Display Firmware Status (DSPFMWSTS) command to determine the i5/OS product and release for server firmware PTFs.

Downloading an update to an FTP server

Find out how to download an update to an FTP server.

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 update to the FTP server. Second, you use the HMC interface to install the update from the FTP server to the HMC.

To download an HMC update to an FTP server, follow these steps:

1. Go to the Fix Central Web site at <http://www.ibm.com/eserver/support/fixes/> .
2. Click the appropriate family in the Server list.
3. Click **Hardware Management Console** in the Product or fix type list.
4. Click **Continue**. Information on HMC update is displayed.
5. After you have downloaded the update from the Web site to your FTP server, continue with the procedure that sent you here.

Related information

 [Fix Central Web site](#)

Removing the current firmware level

Find out how to remove the current level of firmware so you can return to a previous level of server firmware or power subsystem firmware.

You can remove the current level of firmware (Licensed Internal Code) if you want to return to a previous level. Use one of the following methods to remove the current level of server or power subsystem firmware, depending on your service environment.

Using an HMC to remove the current firmware level:

Find out how to remove the current level of firmware with an HMC so you can return to a previous level of server firmware or power subsystem firmware.

To remove the current level of 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 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 usual procedures to shut down the logical partitions:

- To shut down i5/OS logical partitions, use the Power Down System (PWRDWN SYS) 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.
- To shut down AIX logical partitions, see Shutting down AIX.
- To shut down Linux logical partitions, see Shutting down Linux.

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

Related information

Shutting down AIX logical partitions

 Power Down System (PWRDWN SYS)

Shutting down i5/OS logical partitions

Shutting down Linux logical partitions

Using AIX commands and tools to remove the current server firmware level:

Find out how to remove the current level of server firmware when you are using AIX.

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

- Using the diagnostic service aids to remove the current firmware level
- Using the `update_flash` command

Using the diagnostic service aids to remove the current firmware level

Note: To perform this task, you must meet the following criteria:

- You must have root user authority.
 - You must start your server from the *permanent* side. For details, see Working with the temporary and permanent side of the service processor.
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_005.
The current temporary system firmware image is SF220_006.
The system is currently booted from the permanent image.

Validate and Update System Firmware
Update System Firmware
Reject the Temporary Image
```
6. Select **Reject the Temporary Image**, and press Enter.

Using the `update_flash` command to remove the current firmware level

Note: To perform this task, you must meet the following criteria:

- You must have root user authority.
- You must start your server from the *permanent* side. For details, see Working with the temporary and permanent side of the service processor.

Type the following at an AIX command line:

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

Related tasks

“Working with the temporary and permanent side of the service processor” on page 208

Find out how to determine which side you are booting from, and how to switch to the other side if necessary.

Using the Linux command line to remove the current server firmware level:

Find out how to use the Linux command line to remove the current level of firmware.

Note: To perform this task, you must meet the following criteria:

- You must have root user authority.
 - You must start your server from the *permanent* side. For details, see Working with the temporary and permanent side of the service processor.
1. Ensure you have the following service tools installed on your server:
 - Platform Enablement Library – `librtas-xxxxx.rpm`
 - Service Aids – `ppc64-utils-xxxxx.rpm`

Note: The `xxxxx` represents a specific version of the RPM file.

2. Choose from the following options:
 - If you do not have the service tools on your server, refer to Obtaining service and productivity tools for Linux.
 - After the service tools are installed to the server or partition running Linux, type the following at a Linux command line:

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

Related tasks

“Working with the temporary and permanent side of the service processor” on page 208
Find out how to determine which side you are booting from, and how to switch to the other side if necessary.

“Obtaining service and productivity tools for Linux” on page 207
Find out about obtaining service and productivity tools for Linux.

Using IBM i5/OS to remove the current server firmware level:

You can remove the current level of firmware when you are using i5/OS so you can return to a previous level of server firmware.

To remove the current level of server firmware when you are using i5/OS, you need to identify the PTFs that correspond to the server firmware fixes.

Refer to the following:

- For details on viewing the existing level of firmware, see “Using IBM i5/OS to view the installed server firmware PTFs” on page 189.
- For details on removing software fixes, see Removing software fixes in the i5/OS Information Center.

Notes:

- If you are using Licensed Internal Code V5R4M0, the PTFs for server firmware are displayed with the Licensed Internal Code product (5722999) and begin with the prefix MH. For example, MHnnnnn where nnnnn is the number associated to the specific server firmware fix.
- If you are using Licensed Internal Code V5R4M5, use the Display Firmware Status (DSPFMWSTS) command to determine the i5/OS product and release for server firmware PTFs.

When you shut down the i5/OS service partition to remove 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 or removed. Allow the server to complete the processing; do not interrupt this process.

Applying an earlier level of server firmware after exchanging the service processor in a model 570 or 9116-561

After a service processor is replaced in a model 570 or 9116-561, it might be a certification requirement to stay at the earlier level of server firmware.

Only apply an earlier level of server firmware if is a certification requirement to use an earlier level of server firmware.


Using an HMC to apply an earlier level of server firmware after exchanging the service processor in a model 570 or 9116-561:

Learn how to use the HMC to apply an earlier level of server firmware if it is a certification requirement.

Only apply an earlier level of server firmware when it is a certification requirement to use an earlier level of server firmware.

If you have an Internet connection from your system, you will be able to download the earlier level of firmware during this procedure.

If you need to obtain the server firmware level on CD, refer to the Fix Central Web site at

<http://www.ibm.com/eserver/support/fixes/>  and follow the prompts to download the update to a system with an Internet connection. You can then create a CD and bring it to this system.

Important: If the HMC machine code is V5R1.1 or earlier, a CD or DVD must be used, and the CD or DVD must contain only the firmware level that is to be loaded on the service processor. No other firmware should be on the CD or DVD.

1. To apply an earlier level of server firmware with an HMC, expand the **Licensed Internal Code Maintenance** folder.
2. Click the **Licensed Internal Code Updates** icon.
3. To apply an earlier release, click **Upgrade Licensed Internal Code to a new release** in the Contents area.
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 apply an earlier level of server firmware.
5. In the Specify LIC Repository window, select the repository location from which you want to download the server firmware, and click **OK**.

Note: If the HMC machine code is V5R1.1 or earlier, a CD or DVD must be used.
The following options are available:

- **IBM service Web site:** (This site provides the most recent level of updates. You need a direct Internet connection to access this site.)
- **IBM support system** (This site provides all available levels of updates. You can use a modem or direct Internet connection to access this site.)

Note: Downloading server firmware updates over a modem might take several hours.

- **DVD-RAM media:** Select this option if you previously put the update on CD and it is in the DVD drive on the HMC.

Notes:

- If the HMC machine code is V5R1.1 or earlier, a CD or DVD must be used, and the CD or DVD must contain only the firmware level that is to be loaded on the service processor. No other firmware should be on the CD or DVD.
- If you choose the DVD-RAM media repository and receive an I/O Error when using a CD that you created, it might mean that the software you used to create the CD does not conform to the writing of temporary records requirements of the HMC.
- **FTP site:** Select this option if you previously downloaded the update to an FTP site. (This site would be setup previously by your organization's advanced support personnel.) An FTP server is any system on which the FTP server protocol is activated. If you select the FTP site, you need to know the following information:

Note: Usually, a PC has only the FTP client active.

- **FTP site** - The fully qualified host and domain name of the FTP server from which you want to download the update.
 - **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 update. You can specify the default directory /opt/ccfw/data if you placed the update in that directory, or you can change the directory path if the update is in a directory other than the default directory. For example, if you downloaded the update and copied it to a unique directory on the FTP server, you can specify that directory.
6. In the License Agreement window, read the agreement and click **Accept**.
 7. In the Confirm the Action window, perform the required actions, and click **Finish**.
 8. To verify that the level of server firmware is the earlier level you applied, on the ASMI Welcome pane, view the existing level of server firmware in the upper-right corner below the copyright statement, for example, SF230_156.

Using AIX or Linux commands to apply an earlier level of server firmware after exchanging the service processor in a model 570 or 9116-561:

Learn how to use AIX or Linux commands to apply an earlier level of server firmware if it is a certification requirement.

Only apply an earlier level of server firmware when it is a customer certification requirement to use an earlier level of server firmware.

Refer to Obtaining server firmware updates through AIX or Linux without an HMC. The steps to apply an earlier level of server firmware is the same as applying a later level. You will need to select the appropriate level during the procedure.

Related tasks

“Obtaining server firmware updates through AIX or Linux without an HMC” on page 160
Learn how to obtain updates to server firmware through AIX or Linux without an HMC.

Using i5/OS commands to apply an earlier level of server firmware after exchanging the service processor in a model 570 or 9116-561:

Learn how to use i5/OS commands to apply an earlier level of server firmware if it is a certification requirement.

Only apply an earlier level of server firmware when it is a customer certification requirement to use an earlier level of server firmware.

Refer to “Obtaining server firmware updates through IBM i5/OS” on page 166. The steps to apply an earlier level of server firmware is the same as applying a later level. You will need to select the appropriate level during the procedure.

Troubleshooting firmware updates

Find solutions to problems that you might have while applying a server or power subsystem firmware update.

HMC system information panel shows all zeros

Use this procedure to find out what to do when the system information panel shows all zeros in the fields for *installed*, *activated*, and *accepted levels*.

1. Determine the current level of server firmware using the ASMI or the operating system. See Viewing existing firmware levels.
2. Determine the current flash side by issuing the following command from the command line.
`lssyscfg -r sys`
3. Record the information that is displayed in the results for `curr_power_on_side` (either temp or perm). You will need this information later in this procedure.
4. Prepare the managed system to shut down and restart on the other service processor flash side by performing these steps:
 - a. Expand the **Licensed Internal Code Maintenance** folder.
 - b. Click the **Licensed Internal Code Updates** icon.
 - c. In the contents area, click **Flash Side Selection**.
 - d. To shut down and restart to the other flash side of the service processor: In the Flash Side Selection window, select **p-side** or **t-side** based on the information recorded in step 3. If you recorded temp, select p-side, if you recorded perm, select t-side.
 - e. Click **OK**.
 - f. In the Confirm Flash Side Selection window, click **OK**.

5. Restart the managed system.

Note: This process is disruptive. You need to manually shut down all the applications and logical partitions to prevent the system from shutting them down abnormally during the process.

Use the usual procedures to shut down the logical partitions:

- To shut down AIX logical partitions, see Shutting down AIX logical partitions.
 - To shut down i5/OS logical partitions, use the Power Down System (PWRDWN SYS) command from an i5/OS command line (either in a 5250 emulator session on your HMC, or on the Operations Console). For further details, see Shutting down i5/OS logical partitions.
 - To shut down Linux logical partitions, see Shutting down Linux logical partitions.
6. Perform a disruptive activate from the HMC:
 - a. Expand the **Licensed Internal Code Maintenance** folder.
 - b. Click the **Licensed Internal Code Updates** icon.
 - c. In the Contents area, click **Change Internal Code**.
 - d. In the Target Object Selection window, click the target system, and click **OK**.
 - e. In the Change Internal Code window, select **Select advanced features**, and click **OK**.
 - f. In the Advanced Features window, select **Disruptive activate**, and click **OK**. At the end of a disruptive process, the managed system automatically returns to its original state.
 7. After the system restarts, use the HMC's system information panel to determine the activated level. Refer to Viewing existing firmware (Licensed Internal Code) levels.
 8. Choose from the following options:
 - If the activated level is still 0, then there is a problem with both flash sides. Contact your next level of support to proceed.
 - If the activated level is a level other than 0, you can use the advanced feature "Install and activate (implied Retrieve)" option to install either the highest level or the specific update level you want. For details, see Obtaining a specific firmware update with an HMC.

Related tasks

"Viewing existing firmware levels" on page 186

Find out how to view the level of firmware that currently runs on your server.

Related information

Shutting down AIX logical partitions

 Power Down System (PWRDWN SYS)

Shutting down i5/OS logical partitions

Shutting down Linux logical partitions

Message regarding a server that was previously managed by an HMC

Use this procedure to find out what to do if you receive a message regarding a server that was previously managed by an HMC.

The following message might be displayed if you previously used an HMC to manage the server, but you disconnected the HMC because you no longer want to use the HMC to manage the server:

This partition does not have the authority to perform the requested function. Verify that this partition has service authority. If the problem persists after granting the partition service authority, then contact your service support structure.

In this situation, you need to perform the following tasks to solve the problem:

1. If you have logical partitions, ensure that one of your logical partitions is designated to be a service partition for the managed system. For more information, see Designating the service partition for your managed system.

2. Change the firmware update policy from **Hardware Management Console (HMC)** to **Operating System**. For instructions about how to change the policy, see [Changing the firmware update policy](#).

Note: For more information on disconnecting a managed system from an HMC, see [Deleting a managed system](#).

Related information

[Designating the service partition for your managed system](#)

[Changing the firmware update policy](#)

[Deleting a managed system](#)

Obtaining server firmware updates through AIX or Linux when you are unable to start the operating system or server

Learn how to apply server firmware updates through AIX or Linux when you are unable to start the operating system or server.

The server firmware is the part of the Licensed Internal Code that enables hardware, such as the service processor.

Note: Installing the server firmware updates through the operating system is a disruptive (nonconcurrent) process.

Perform Steps 1 through 4.

Related tasks

[“Running the eServer stand-alone diagnostics from CD-ROM” on page 408](#)

If the system or logical partition where you would like to run diagnostics has AIX installed but it cannot be started, or you have Linux installed, use this procedure to perform diagnostic procedures from CD-ROM when directed from another procedure or by your next level of support.

Step 1. Determine the existing level of firmware:

Use this procedure to determine the existing level of server firmware when you are unable to start the AIX or Linux operating system or server.

1. Insert the eServer Standalone Diagnostics Version xxxxx CD into the CD drive on the server and boot the CD. If you need more information about how to boot the Standalone Diagnostics Version xxxxx CD, see [Running the eServer stand-alone diagnostics from CD](#).
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**

Note: When the lsmcode command is run on a 7037-A50 or 7047-185 system, the temporary or permanent side of the flash might report `_UNKNOWN_` for the firmware level. This occurs because there is only one level of base motherboard controller firmware. The level is `_UNKNOWN_` when it is not included with the system firmware.

When you install new firmware, it is installed onto the temporary side by default. This new firmware level includes a new level of base motherboard controller code, and will cause `_UNKNOWN_` to be reported for the permanent side. This is not a problem; it indicates that the firmware levels in the flash are not a combination that is included from the factory.


To update the firmware so that `_UNKNOWN_` is not reported, perform the following steps:

- a. Perform a commit operation using the appropriate operating system command.
- b. After the commit operation is complete, restart the system.

- c. When the system has restarted and the operating system is running, rerun the `lsmcode` command. Both the T and P should report a level (such as AT206_061) instead of `_UNKNOWN_`.
5. Record the information for the current temporary system firmware image.

Step 2. Obtain the Microcode Update Files & Discovery Tool CD:

You will need to obtain the *Microcode Update Files & Discovery Tool* CD. Contact service and support for details.

1. From a computer or server with an Internet connection, go to the Fix Central Web site at <http://www.ibm.com/eserver/support/fixes/> 
2. Select the appropriate family in the Product family list.
3. Select **Hardware microcode and firmware** in the Product list.
4. Click **Continue**.
5. Perform the following steps:
 - a. Follow the on-screen prompts to download the image.
 - b. Follow the instructions for your CD program to create the CD.
 - c. After you have the CD, continue with "Step 3. Apply the server firmware update."

Step 3. Apply the server firmware update:

1. Insert the *Microcode Update Files & Discovery Tool* CD into the media device, select **Validate and Update System Firmware**, and press Enter.

Note: If you receive a message stating: This partition does not have the authority to perform the requested function, see Message regarding a server that was previously managed by an HMC.

2. Select the appropriate device and press Enter.
3. Press F4. A list of firmware update image files is displayed.
4. Select the image file that is similar to `/microcode/SqnP5/01SF2xx_yyy_zzz.img`.
5. Press F7. The server firmware level that you selected will be installed on the temporary side.

Related tasks

"Message regarding a server that was previously managed by an HMC" on page 201
Use this procedure to find out what to do if you receive a message regarding a server that was previously managed by an HMC.

Step 4. Verify that the update installed correctly:

Use this procedure to verify the update installed correctly.

1. Choose from the following options:
 - To use the AIX or Linux command prompt (the operating system must be running and the diagnostics must be available), continue with the next step.
 - To use the ASMI, view the level of server firmware displayed in the upper-right corner below the copyright statement on the ASMI Welcome pane; for example, SF220_006. If the level of server firmware displayed is not the level that you installed, refer to step 5 on page 204.
2. Enter the following at a command prompt:


```
lsmcode
```

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

```
The current permanent system firmware image is SF220_005.
The current temporary system firmware image is SF220_006.
The system is currently booted from the temporary image.
```

Note:

- a. The permanent level is also known as the backup level.
 - b. The temporary level is also known as the installed level.
 - c. The system was booted from the temporary side, so at this time the temporary level is also the activated level.
3. If you are using a 7037-A50 or 7047-185 system, note the following:

Note: When the `lsmcode` command is run on a 7037-A50 or 7047-185 system, the temporary or permanent side of the flash might report `_UNKNOWN_` for the firmware level. This occurs because there is only one level of base motherboard controller firmware. The level is `_UNKNOWN_` when it is not included with the system firmware.

When you install new firmware, it is installed onto the temporary side by default. This new firmware level includes a new level of base motherboard controller code, and will cause `_UNKNOWN_` to be reported for the permanent side. This is not a problem; it indicates that the firmware levels in the flash are not a combination that is included from the factory.

To update the firmware so that `_UNKNOWN_` is not reported, perform the following steps:

- a. Perform a commit operation using the appropriate operating system command.
 - b. After the commit operation is complete, restart the system.
 - c. When the system has restarted and the operating system is running, rerun the `lsmcode` command. Both the T and P should report a level (such as `AT206_061`) instead of `_UNKNOWN_`.
4. Verify that the level of server firmware displayed is the level that you installed.
5. If the level of server firmware displayed is not the level that you installed, perform the following steps:
- a. Retry the update. If you created a CD or DVD for this procedure, use a new media.
 - b. If the problem persists, contact your next level of support.

Additional information about obtaining updates


Find additional information about obtaining updates.

Using the AIX diagnostics to install the server firmware update through AIX

Use this procedure if you want to use the AIX diagnostics to install the server firmware update through AIX to the temporary side of the service processor.

Note: If you plan to install the update from CD using the AIX diagnostics, you will need to obtain the *Microcode Update Files & Discovery Tool* CD. The instructions are included in the procedure.

To install the server firmware update using the AIX diagnostics, follow these steps:

1. Choose from the following options:
 - If you plan to install the update from your hard drive, continue with step 9 on page 205.
 - If you need to create the *Microcode Update Files & Discovery Tool* CD, continue with step 2.
2. From a computer or server with an Internet connection, go to the Fix Central Web site at <http://www.ibm.com/eserver/support/fixes/> .
3. Select the appropriate family in the Product family list.
4. Select **Hardware microcode and firmware** in the Product or fix type list.
5. Click **Continue**. The Microcode downloads Web site appears.
6. Follow the on-screen prompts to download the image.
7. Follow the instructions for your CD program to create the CD.

8. Insert the CD into the CD drive on your server.
9. At the AIX command prompt, enter the following:
diag
10. Initialize the terminal type, if requested.
11. On the function selection screen, select **Tasks and Service Aids**.
12. On the task selection screen, scroll to the bottom of the list of options, and select **Update and Manage Flash**. 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_006.
The system is currently booted from the temporary image.

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

13. Select **Validate and Update System Firmware**, and press Enter. A screen similar to the following is displayed:

UPDATE AND MANAGE SYSTEM FLASH

This service aid updates the system firmware. The flash update image file is copied from the source selected below, to the file /var/update_flash_image. Then the system is rebooted to perform the flash update.

Select the source of the flash update image file:

Removable Media
File System

Note: If you receive a message stating: This partition does not have the authority to perform the requested function, see Message regarding a server that was previously managed by an HMC. During the server firmware installation process, reference codes CA2799FD and CA2799FF are alternately displayed on the control panel. After the installation is complete, the system is automatically powered off and powered on.

14. Choose from the following options:
 - a. If the update is located on your hard drive, continue with step 15.
 - b. If the update is located on a CD, continue with step 19.
15. Select **File System**. A screen similar to the following is displayed.

UPDATE AND MANAGE SYSTEM FLASH

Enter the fully qualified path name of the file with the flash update image. The file will be copied to /var/update_flash_image.

When finished, use 'Commit' to continue.

flash update image file

[]

16. Enter the fully qualified path name of the file with the flash update image. The file will be copied to the /var/update_flash_image directory.
17. When finished, select **Commit**. The server firmware level that you selected will be installed on the temporary side.
18. Continue with step 24 on page 206.
19. Insert the *Microcode Update Files & Discovery Tool* CD that contains the .img update file into the media drive on your server and select **Removable Media**. A screen similar to the following is displayed:

UPDATE AND MANAGE SYSTEM FLASH

This service aid updates the system firmware.
The file must be on removable media to update the flash.
The flash update image file is copied from the media,
then the system is rebooted to perform the flash update.
Select the device containing flash update image files.
Make selection, use 'Enter' to continue.
/dev/cd0
/dev/cd1

Note: If you receive a message stating: This partition does not have the authority to perform the requested function, see “Message regarding a server that was previously managed by an HMC” on page 201.

20. Select the appropriate device and press Enter. A screen similar to the following is displayed:

UPDATE AND MANAGE SYSTEM FLASH

Enter the flash update image file on the device. The file
will be copied to /var/update_flash_image.

When finished, use 'Commit' to continue.

flash update image file [/microcod> +

21. Press F4. A list of firmware update image files is displayed.
22. Select the image file that is similar to: /microcode/SqnP5/01SF2xx_yyy_zzz.img.
23. Press F7. The server firmware level that you selected will be installed on the temporary side.
24. To verify that the server firmware update installed successfully, see “Step 5. Verify that the update installed correctly” on page 165 in “Obtaining server firmware updates through AIX or Linux without an HMC” on page 160.
25. If you want to install the update permanently, refer to “Step 6. (Optional) Install the server firmware update permanently” on page 165 in “Obtaining server firmware updates through AIX or Linux without an HMC” on page 160.

Related tasks

“Message regarding a server that was previously managed by an HMC” on page 201

Use this procedure to find out what to do if you receive a message regarding a server that was previously managed by an HMC.

Using the System Management Interface Tool to mount the update CD for AIX

Use this procedure if you want to use SMIT to mount the update CD for AIX.

If you are applying a server firmware update through AIX and receive a message regarding mounting the CD, mount: 0506-324 Cannot mount /dev/cd0 on /mnt, use this procedure to correct the problem.

1. At an AIX command line, type one of the following commands depending on whether you use a graphics terminal or an ASCII terminal:
 - If you use a graphics terminal, type the following command:
smit
 - If you use an ASCII terminal, type the following command:
smitty

Note: If you are unfamiliar with the System Management Interface Tool (SMIT), select **Using Smit (information only)** for information about how to use SMIT.

2. On the System Management screen, select **System Storage Management (Physical and Logical Storage)**.

3. On the System Storage™ Management (Physical and Logical Storage) screen, select **File Systems**.
4. On the File Systems screen, select **Mount a File System**.
5. On the Mount a File System screen, specify the following values in the entry fields, and press Enter. Do not press Enter until you specify values in all of the required fields.

Table 3. Descriptions and entry field values in the System Management Interface Tool (SMIT)

Description	Entry Field
FILE SYSTEM name	/dev/cd0
DIRECTORY over which to mount	/mnt
TYPE of file system	cdrfs
FORCE the mount?	yes
REMOTE NODE containing the file system to mount	Note: Leave this field blank.
Mount as a REMOVABLE file system?	yes
Mount as a READ-ONLY system?	yes
Disallow DEVICE access via this mount?	no
Disallow execution of SUID and sgid programs in this file system?	no

6. To exit SMIT, press F3 several times or press F10.
7. To verify that the CD mounted successfully, type the following at an AIX command line:

```
mount
```

If the CD mounted successfully, a line of output similar to the following is displayed along with the date and time:

```
/dev/cd0 /mnt cdrfs
```
8. Choose from the following options:
 - If the output is displayed, continue with the next step.
 - If the output is not displayed, repeat steps 2 on page 206 through 7.
9. Continue with step 6 in “Step 3. View and unpack the RPM file that contains the server firmware” on page 162 in “Obtaining server firmware updates through AIX or Linux without an HMC” on page 160.

Obtaining service and productivity tools for Linux

Find out about obtaining service and productivity tools for Linux.

While performing firmware updates, running diagnostics, or running other commands at a Linux command line, you might need to have service and productivity tools installed for Linux. These tools might include the following:

- **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.

If your server *is not* connected to the Internet, download the service tools to a PC or server that is connected to the Internet and burn a CD that contains the service tools. Next, you install the service tools from the CD to the server.

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

1. Go to the Service and productivity tools for Linux on POWER® Web site.
2. Click your Linux distributor.
3. Click the RPM file for the service tool.

4. 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.

5. In the File Download window, click **Save**, specify the directory to which you want to download the RPM file, and click **Save**.
6. Choose from the following options:
 - If you are installing the file directly to the server, continue with step 10.
 - If you are creating a CD, continue with the next step.
7. Follow the instructions for your CD program to create the CD.
8. Insert the CD into the media drive on your server.
9. To mount the CD, type one of the following commands at a Linux command line:

```
mount -t iso9660 /dev/cdrom /mnt
```

or

```
mount -t iso9660 /dev/dvdrom /mnt
```

10. To install 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 filename.rpm
```

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

11. Choose from the following options:
 - If the server *is* connected to the Internet, this ends this procedure.
 - If the server *is not* connected to the Internet, unmount the CD by typing the following at a Linux command line:

```
umount /mnt
```

Related information



Service and productivity tools for Linux on POWER

Working with the temporary and permanent side of the service processor

Find out how to determine which side you are booting from, and how to switch to the other side if necessary.

Using the HMC to work with the temporary and permanent side of the service processor:

Learn how to use the HMC to determine which side of the service processor you are booting from.

Note: You should usually be running on the Temporary side.

1. From the HMC command line, issue the following command:


```
lssyscfg -r sys
```
2. Identify the managed system you are working with by looking for the system number at the beginning of the block of output, and look for this parameter: *curr_power_on_side*.
3. Record the information that is displayed in the results for *curr_power_on_side* (either temp or perm). You will need this information later in this procedure if you decide to change the boot side.
4. If you need to change the boot side, continue with the next step.

5. Expand the **Licensed Internal Code Maintenance** folder.
6. Click the **Licensed Internal Code Updates** icon.
7. In the contents area, click **Flash Side Selection**.
8. Indicate to shut down and restart to the other flash side of the service processor. In the Flash Side Selection window, select **p-side** or **t-side** based on the information you recorded earlier. If you recorded temp, select p-side, if you recorded perm, select t-side.
9. Click **OK**.
10. In the Confirm Flash Side Selection window, click **OK**.
11. Shut down and restart the managed system using the usual procedures to shut down the logical partitions:

Note: This process is disruptive. You need to manually shut down all the applications and logical partitions to prevent the system from shutting them down abnormally during the process.

- To shut down AIX logical partitions, see Shutting down AIX 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 details, see Shutting down i5/OS logical partitions.
- To shut down Linux logical partitions, see Shutting down Linux logical partitions.

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

12. Perform a disruptive activate from the HMC by completing the following steps.
 - a. Expand the **Licensed Internal Code Maintenance** folder.
 - b. Click the **Licensed Internal Code Updates** icon.
 - c. In the Contents area, click **Change Internal Code**.
 - d. In the Target Object Selection window, click the target system, and click **OK**.
 - e. In the Change Internal Code window, select **Select advanced features**, and click **OK**.
 - f. In the Advanced Features window, select **Disruptive activate**, and click **OK**.

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

Related information

Shutting down AIX logical partitions

 Power Down System (PWRDWNSYS)

Shutting down i5/OS logical partitions

Shutting down Linux logical partitions

Using AIX or Linux commands to work with the temporary and permanent side of the service processor:

Learn how to use AIX or Linux commands to determine which side of the service processor you are booting from.

Note: In most cases, you will be running on the Temporary side.

1. Issue the following command at the AIX or Linux command prompt:

```
lsmlcode
```

Note: If the lsmlcode command does not work on the Linux command line, you need to obtain the Linux tools. See Obtaining service and productivity tools for Linux.

2. Record the information that is displayed. You will need this information later in this procedure if you need to change the boot side. The information that is displayed is similar to:
 - AIX: The system is currently booted from the xx image (either temporary or permanent).

- Linux: The (b) booted side shows whether the firmware matches the temporary or permanent side code.

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

3. If you need to change the boot side, refer to “Switching to the other side of the service processor using ASMI or the control panel.”

Related tasks

“Obtaining service and productivity tools for Linux” on page 207

Find out about obtaining service and productivity tools for Linux.

Using the IBM i5/OS tools to work with the temporary and permanent side of the service processor:

Learn how to use i5/OS tools to determine which side of the service processor you are booting from.

Note: You should usually be running on the Temporary side.

1. Issue the following command from the i5/OS service partition command line:

DSPPTF

2. Record the information that is displayed in the IPL source field. You will need this information later in this procedure if you need to change the boot side. The following is an example of what might appear:

Display PTF Status		System:	xxxxxxx
Product ID	:	5722999
IPL source	:	##MACH#B ##SERV#T
Release of base option	:	V5R3M0 L00

Note the following:

- A value of ##SERV#T indicates the temporary side was used.
- A value of ##SERV#P indicates that the permanent side was used.

Note: If the command does not work, ensure you are on the service partition of an IBM System i5 or eServer i5.

3. If you need to change the boot side, refer to “Switching to the other side of the service processor using ASMI or the control panel.”

Using the control panel to work with the temporary and permanent side of the service processor:

Learn how to use the control panel to switch to the other side of the service processor, if necessary.

In most cases, you will be running on the Temporary side.

Follow these steps to change the boot side and shut down and restart the system using the control panel:

1. On the control panel, press the increment button until 02 is shown on the Function/Data display.
2. Record whether a T or P is shown.
3. If you need to change the boot side, refer to “Switching to the other side of the service processor using ASMI or the control panel.”

Switching to the other side of the service processor using ASMI or the control panel:

Learn how to use the ASMI or the control panel to switch to the other side of the service processor, if necessary.

Using the ASMI to switch to the other side of the service processor:

Learn how to use the ASMI to switch to the other side of the service processor, if necessary.

Note:

1. You should usually be running on the Temporary side.
2. If you are working on a 7037-A50 or 7047-185 system, use control panel function 02 to switch to the other side of the firmware flash memory. For details, see *Using the control panel to switch to the other side of the service processor*.

Note: You can also use the Power/Restart Control menu in the SMS menus to switch to the other side of the firmware flash memory.

Follow these steps to change the boot side and shut down and restart the system using the ASMI:

1. Use the normal procedures to shut down the logical partitions.

Note: This process is disruptive. You need to manually shut down all the applications and logical partitions to prevent the system from shutting them down abnormally during the process.

- To shut down AIX logical partitions, see *Shutting down AIX logical partitions*.
 - To shut down i5/OS logical partitions, use the Power Down System (PWRDWN SYS) command from an i5/OS command line (either in a 5250 emulator session on your HMC, or on the Operations Console). For further details, see *Shutting down i5/OS logical partitions*.
 - To shut down Linux logical partitions, see *Shutting down Linux logical partitions*.
2. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
 3. In the navigation area, expand Power/Restart Control and select **Power On/Off System**.
 4. In the Firmware boot side for the next boot field, indicate to boot to the other boot side of the service processor. Select **Permanent** or **Temporary** based on the information you recorded earlier. If you recorded temp or #T, select Permanent, if you recorded perm or #P, select Temporary.
 5. Choose one of the following to shut down and restart the managed system based on the state of the server:
 - Click **Save settings** to save the selected options. The power state does not change.
 - Click **Save settings and power on/off**. All selected options are saved and the system turns on or off. The power-on option is available only if the system is powered off. The power-off option is only available if the system is powered on.
 - Click **Save settings and continue server firmware boot** to save the selected options, and turn the server firmware on or off. The option is available only if the server firmware is in *standby* mode.

Related tasks

“Using the control panel to switch to the other side of the service processor”

Learn how to use the control panel to switch to the other side of the service processor, if necessary.

Related information

Shutting down AIX logical partitions

 Power Down System (PWRDWN SYS)

Shutting down i5/OS logical partitions

Shutting down Linux logical partitions

Using the control panel to switch to the other side of the service processor:

Learn how to use the control panel to switch to the other side of the service processor, if necessary.

You should usually be running on the Temporary side.

Follow these steps to change the boot side and shut down and restart the system using the control panel:

1. On the control panel, press the increment button until 02 is shown on the Function/Data display.
2. Press Enter until the arrow (<) points to T or P.

3. Press the increment button until the T or P is changed.
4. Press Enter to accept the changes.
5. Shut down and restart the server.

Note: This process is disruptive. You need to manually shut down all the applications and logical partitions to prevent the system from shutting them down abnormally during the process.

- To shut down AIX logical partitions, see Shutting down AIX 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 details, see Shutting down i5/OS logical partitions.
- To shut down Linux logical partitions, see Shutting down Linux logical partitions.

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

Related information

Shutting down AIX logical partitions

 Power Down System (PWRDWNSYS)

Shutting down i5/OS logical partitions

Shutting down Linux logical partitions

Getting started with troubleshooting

Learn how you and your server can manage problems, and ways you can detect that problems have occurred.

Managing problems

Use this information to determine what you should do to manage problems, including how to use your systems to help you manage problems.

Your system provides functions for problem logging, tracking, reporting, analysis, and correction. However, oftentimes you will also need to detect, analyze, and report a problem too.

How you manage problems

Learn about how you can detect, analyze and report a problem.

When your server was purchased, you might have purchased a server with warranty options that enable you or someone in your company to repair the server, even during the warranty period. Use the following list to determine your troubleshooting and service course of action.

1. You might receive an indication that your server has a problem. For example, the system attention light comes on or you receive notification of a problem. Sometimes you might sense something is wrong without any precise indication. For more details, see Attention light overview.
2. You perform procedures to determine the source of the problem, find possible recovery actions, and gather detailed information about the problem. See Beginning problem analysis.
3. If you are unable to correct the problem, contact your next level of support or your service provider. For details, see Contacting IBM service and support.
4. If your service provider is contacted, one of the following will occur:
 - If the service action is a customer responsibility, you will be instructed to take the appropriate action. If a part needs to be replaced that is customer-replaceable, it will be included with a pointer to the installation instructions. For details, see Installing features.
 - If the service action requires an IBM service representative or other service provider, the call is directed to the service representative.

If you performed a service action, you will be directed to the appropriate verification procedure.

Related concepts

“Attention light overview” on page 214

Learn more about the attention light and how you can use it to identify a problem.

“Contacting IBM service and support” on page 447

Use this information to learn how to contact the IBM service and support organization.

Related tasks

“Beginning problem analysis” on page 219

Start here to determine what caused a problem and learn how to recover from it.

How your system manages problems

Learn how your system can provide functions for problem logging and tracking, reporting, analysis, and correction.

Your system provides functions for problem logging and tracking, problem reporting, problem analysis, and problem correction. The problem management process helps you and your service provider quickly and accurately manage problems as they occur on the system.

Note: In this topic, **control panel** and **operator panel** are synonymous.

Here is an example of the flow when managing a problem:

1. The server or operating system detects an error.
2. A problem record is created with configuration information, a reference code, the name of the reporting device, and other information.
3. The error is recorded.
4. One or more of the following events will occur:
 - An error notification is sent to the system console. Possible consoles include the following:
 - Hardware Management Console (HMC)
 - Advanced System Management Interface (ASMI)
 - Integrated Virtualization Manager
 - Operations Console
 - Twinaxial console
 - ASCII terminal
 - If you configured the e-mail notification option, an e-mail notification is sent to a designated user. You can enable e-mail notification by using the Electronic Service Agent on the HMC. For more details, see Electronic Service Agent .
 - The system attention light comes on.
 - A reference code might be displayed on the control panel or on the HMC.
 - If you are using an HMC, a serviceable event is shown in the Service Focal Point application on the HMC.
5. After there is a message or reference code available, you can use that information to begin problem analysis. For details, see Beginning problem analysis.

The results of problem analysis are automatically stored, along with the data that was collected. At this point, you can manually report the problem to your hardware service provider, or you can configure your server, HMC, or other console for electronic problem reporting. To learn how to set up your service environment for electronic problem reporting, see Setting up your server to connect to service and support.

Various tools are available to help you manage the problems on your server. See the following information to help you troubleshoot problems on the server:

- Detecting problems

- Reporting problems

Related concepts

“Electronic Service Agent” on page 9

Learn more about the Electronic Service Agent application which monitors your servers after you enable it.

“Setting up your server to connect to service and support” on page 31

Learn about setting up your server to connect to service and support.

“Detecting problems”

Learn how to detect problems that have occurred on your system by using the attention light, messages, and reference codes.

“Reporting problems” on page 442

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

Related tasks

“Beginning problem analysis” on page 219

Start here to determine what caused a problem and learn how to recover from it.

Detecting problems

Learn how to detect problems that have occurred on your system by using the attention light, messages, and reference codes.

Attention light overview

Learn more about the attention light and how you can use it to identify a problem.

The attention indicator is activated whenever server firmware or logical partitions detect an event that is logged as a service action. The service action might be correctable by the system administrator, or it might require involvement of a service provider to do problem determination or exchange parts. The attention indicator is therefore a visual prompt to check the serviceable event logs.

All serviceable events will activate the attention indicator, and will prompt notification functions (if this feature is configured) in the operating systems or the HMC depending on where the error occurred, and if the server is managed by an HMC.

The diagnostics in the server’s firmware and in the operating systems determine if the event is severe enough that it should be reported to service and support, if electronic reporting has been configured. All serviceable events cause the attention indicator to be activated and the notification function to be prompted, including pager or e-mail, if it has been configured. Serviceable events that require a service provider will automatically prompt an electronic problem report to service and support if electronic problem reporting to service and support is configured.

Examples of serviceable events that activate the attention indicator but do not prompt electronic problem reporting include:

Note: These events will not automatically trigger electronic problem reporting to service and support but through the operating system or HMC, but the system administrator can choose to have the problems electronically reported if the electronic reporting function has been configured.

- Configuration errors, such as I/O adapters in the wrong slot.
- Ambient air temperature problems.
- Loss of communication between the server and the HMC where the most likely cause is a network problem
- An IBM i5/OS logical partition is posting an attention system reference code.

Examples of serviceable events that activate the attention indicator and will prompt electronic problem reporting:

- Adapter and device failures in an operating system
- Power supply failures in the server and I/O expansion units

The system attention indicator is designed to be activated when a serviceable event occurs and thereby provide a visual indication that the serviceable event logs have a new event. The administrator can then deactivate the system attention indicator using the HMC or the operating system depending on your environment. This allows the administrator to be alerted to a new problem if a new problem occurs. It is not necessary to wait until a problem is resolved before deactivating the system attention indicator. Deactivation is at the administrator's discretion.

To deactivate the attention light, refer to the following:

- To use the HMC, see *Activating and deactivating LEDs*.
- To use the AIX diagnostics, see *Resetting the LEDs in AIX*.

Differences between the server firmware and the operating systems:

- **Serviceable event detected by server firmware:** The system attention indicator is activated and a serviceable event log is passed to the operating systems and to the HMC, if you have one. The HMC will provide notification and electronic problem reporting functions if the system is managed by an HMC. Otherwise, the operating system provides the notification and electronic problem reporting function.
- **Serviceable event detected by AIX and Linux:** The server or logical partition's attention indicator is activated, which also causes the system attention indicator on the server to be activated. The server or logical partition's attention indicator can be deactivated from the console in the diagnostic tools.
 - For HMC managed systems, the logical partition's attention indicator is on the HMC with the logical partition management functions. The serviceable event is sent to the HMC, and the HMC notification and electronic problem reporting functions are triggered.
 - For systems not managed by the HMC, the AIX or Linux notification and problem reporting functions are triggered.
- **Serviceable event detected by i5/OS:** The logical partition's attention indicator is activated, which also causes the system attention indicator on the server to be activated. The logical partitions attention indicator can be deactivated from the partition's console in the SST/DST Service Action Log, under Hardware Service Manager, by Acknowledging the serviceable events.
 - For HMC managed systems the logical partition's attention indicator is on the HMC with the logical partition's management functions. The serviceable event is sent to the HMC. The i5/OS logical partition's notification and electronic problem reporting functions are prompted. This allows the i5/OS automatic fix download functions to be utilized if configured.
 - For systems not managed by an HMC, the i5/OS notification and problem reporting functions are triggered.

There are several examples of why the attention light can be on, and what it might mean:

- If the system attention indicator is on (lit continuously), and there *is not a reference code* displayed in function 11 on the control panel or on the HMC, it means that you have a serviceable event in one of the logical partitions. See *Beginning problem analysis*.
- If the system attention indicator is on (lit continuously), and there *is a reference code* displayed in function 11 on the control panel or on the HMC, it means you need to analyze the problem. See *Beginning problem analysis*.

Where you view the attention light on your server will depend on the model you have. Also, if you have an HMC and your physical attention light illuminates, you will be notified with an attention icon that is displayed over the icon of the server that is affected. If there are logical partitions, the attention icon might also be seen over the logical partition that requires service. The attention icon is a yellow triangle with an exclamation point [!]. When this icon is shown, check the physical attention light to verify that it

is on.

Figure 50. Server icon with the attention light icon



Figure 51. Server icon without the attention light icon



To see where the attention light is shown on your server, choose the model that you are working with:

- All models *except* model 570 and 595
- Model 570

Figure 52. Attention light for all models except model 570 and 595

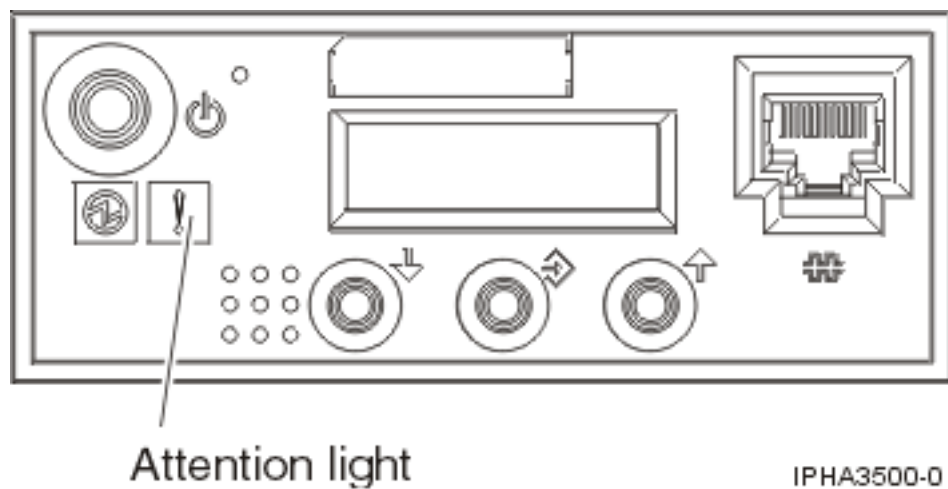
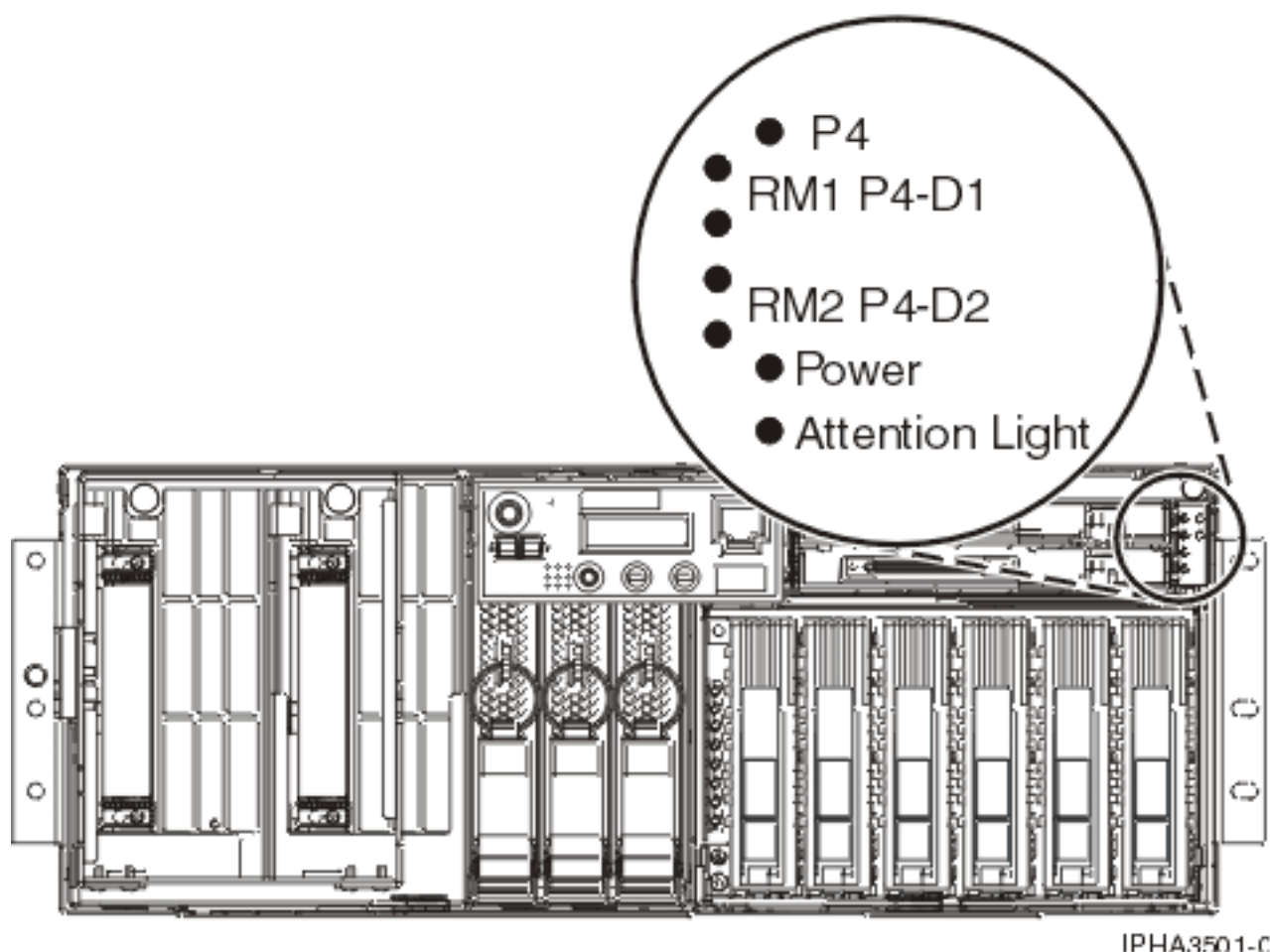


Figure 53. Attention light for model 570



IPHA3501-C

Note: The attention light for the model 570 is located in the upper-right corner, not on the control panel.

Related tasks

“Activating and deactivating LEDs” on page 438

Use this procedure to activate or deactivate LEDs using Service Focal Point for the HMC.

“Beginning problem analysis” on page 219

Start here to determine what caused a problem and learn how to recover from it.

Related information

Resetting the LEDs in AIX

Messages overview

Learn more about messages and how you can use them to identify a problem.

Your server sends informational and inquiry messages that provide you with important system information. Inquiry messages require you to respond. Informational messages allow you to keep track of system activities, jobs, users, and errors. Because messages provide information about your system, you should know how to handle messages when detecting and correcting problems.

Depending on which operating system is reporting the error, and whether you have a Hardware Management Console (HMC), the message is sent to one of the following places:

- AIX error messages are displayed in a window on your console. They also are e-mailed to a specified user or users. By default this is the root user, but notification might be sent to any e-mail address of your choice. You can use the Automatic Error Log and Notification task to configure this. For details, see Viewing AIX messages.

- HMC messages are sent to an e-mail address (if set up) and reported to the Service Focal Point. For details, refer to Using Service Focal Point. To view a list of HMC error codes, see HMC error codes.
- For Linux messages, see Viewing Linux messages.
- i5/OS messages are displayed in a window on your console, or can be viewed in the i5/OS message queue (QSYSOPR). For details, see Viewing IBM i5/OS messages.

Related concepts

“Using Service Focal Point” on page 436

Learn about using the Service Focal Point, an application on the HMC and the Integrated Virtualization Manager, to diagnose and repair problems on the system.

Related tasks

“Viewing AIX messages” on page 434

Learn more about viewing AIX messages.

“HMC error codes” on page 271

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

“Viewing Linux messages” on page 436

Learn more about viewing Linux messages.

“Viewing IBM i5/OS messages” on page 435

Learn more about viewing i5/OS messages.

Reference codes overview

Learn more about the various types of reference codes and how they can help you identify a problem.

Reference codes are diagnostic aids that help determine the source of a hardware or operating system problem. When you perform the procedures in “Beginning problem analysis” on page 219, you will learn how to locate and record the reference codes, which can help you better understand the problem and how to fix it. Also, you might be able to find the code in the “Reference codes list for customers” on page 263 for more information about resolving it.

The following are categories of status indicators that can be displayed in the control panel or console of the system or operating system.

- **Progress codes:** Progress codes (or checkpoints) offer information about the stages involved in powering on and performing an initial program load (IPL). Progress codes do not indicate an error, although in some cases, your server can pause indefinitely (hang). Only when you experience such a hang condition should you take any action based on a progress code. Progress codes appear in several formats:
 - An 8-digit hexadecimal number that begins with a C or D
 - A 3-digit hexadecimal number
 - A 4-digit hexadecimal number that begins with a 0 or 2
- **System reference codes (SRCs):** System reference codes indicate a problem has originated in hardware, in Licensed Internal Code, or in the operating system. A server component generates an error code when it detects a problem. SRCs are strings of either 6 or 8 alphanumeric characters. SRCs appear in the following format:
 - An 8-character code, for example, A2xx1150, except those that begin with a C or D (progress codes) or H (HMC error codes)
 - A 6-character code, for example, xxxxxx, except those that begin with a 0 (HMC error codes)
- **HMC error codes:** The HMC error codes can be displayed in a window on the HMC during system configuration and operations. They contain messages and recovery actions regarding the HMC. They appear in the following formats:
 - A 6-digit error code that begins with 0
 - An 8-digit error code that begins with the letter H

- **Service request numbers (SRNs):** These can be received after performing online or eServer stand-alone diagnostics, or by error log analysis. They are used to determine the source of a hardware or operating-system problem. They are 5 to 8 characters in length, with hyphens appearing in SRNs that are 6, 7, or 8 characters in length (one example is 2600-101). If you receive an SRN, you should record it and contact your next level of support or your hardware service provider for help interpreting what it means.

As a group, these codes are referred to as *reference codes*. The type of code that is shown depends on the operating system you are using and the process you were performing when the code appeared. The codes are either displayed in an error message, recorded in a problem log entry, shown on the system control panel, e-mailed to a designated user, shown on the HMC in a window, or some combination of these. The system attention light might come on if the system detects a hardware error it cannot correct, or when an action is required.

Beginning problem analysis

Start here to determine what caused a problem and learn how to recover from it.

Follow these steps to begin analyzing and handling the problem you are having.

1. Is your server a 7037-A50 or 7047-185?
 - **Yes:** Go to Diagnosing a problem with a 7037-A50 or a 7047-185.
 - **No:** Continue with the next step.
2. Are you troubleshooting the keyboard, video, and mouse (KVM) switch for the 1x8 or 2x8 console manager?
 - **Yes:** Go to “Troubleshooting the keyboard, video, and mouse (KVM) switch for the 1x8 and 2x8 console manager” on page 256.
 - **No:** Continue with the next step.
3. Is there an HMC attached to the failing server?
 - **Yes:** Continue with step 5.
 - **No:** Continue with the next step.
4. Is your system being managed by the Integrated Virtualization Manager?
 - **Yes:** Continue with step 13 on page 220.
 - **No:** Refer to the appropriate procedure:
 - If you are having a problem with an AIX server, go to “AIX problem analysis” on page 221.
 - If you are having a problem with an i5/OS server, go to “IBM i5/OS problem analysis” on page 224.
 - If you are having a problem with a Linux server, go to “Linux problem analysis” on page 232.
5. Is the HMC functional?
 - **Yes:** Continue with the next step.
 - **No:** Refer to “HMC problem analysis” on page 235. Return here after the HMC is functional.
6. Do you have a reference code on the HMC?

Note: For details on viewing reference codes using the HMC, refer to “Collecting reference codes and system information” on page 260.

- **Yes:** Record the reference codes, and refer to “Reference codes list for customers” on page 263 to further isolate the problem.
 - **No:** Continue with the next step to check for serviceable events.
7. In the navigation area of the HMC that is used to manage the server, open **Service Applications** → **Service Focal Point** → **Manage Serviceable Events**.

8. Select the criteria for the serviceable events that you want to view, and click **OK**. The Serviceable Event Overview window opens. The list shows all serviceable events that match your selection criteria. You can use the menu options to perform actions on the serviceable events.
9. Select an event listed in the Serviceable Event Overview window, and select **Selected → View Details**. The Serviceable Event Details window opens showing detailed information about the serviceable event. The upper table shows information, such as problem number and reference code. The lower table shows the field replaceable units (FRUs) associated with this event.
10. Select the Serviceable Event for which you want to view comments and history, and follow these steps:
 - a. Select **View Comments** from the Actions menu. When you are finished viewing the comments, click **Close**.
 - b. Select **View Service History** from the **Actions** menu. The Service History window opens, showing service history associated with the selected error. When you are finished viewing the service history, click **Close**.
11. When you are finished, click **Cancel** twice to close the Serviceable Event Details window and the Serviceable Event Overview window.
12. If you have not determined or resolved the problem, choose from the following options:
 - If you are having a problem with an AIX system or logical partition, continue with “AIX problem analysis” on page 221.
 - If you are having a problem with an i5/OS system or logical partition, continue with “IBM i5/OS problem analysis” on page 224.
 - If you are having a problem with a Linux system or logical partition, continue with “Linux problem analysis” on page 232 “Linux problem analysis” on page 232.
13. Are you able to log on to the Integrated Virtualization Manager interface?
 - **Yes:** Continue with the next step.
 - **No:** Refer to Connecting to the Integrated Virtualization Manager.
14. Did you receive a reference code on the Integrated Virtualization Manager?

Note: For details on viewing reference codes using the Integrated Virtualization Manager, refer to “Collecting reference codes and system information” on page 260.

 - **No:** Continue with the next step to check for serviceable events.
 - **Yes:** Does the reference code begin with B1xx?
 - **No:** Record the reference codes, and refer to “Reference codes list for customers” on page 263 to further isolate the problem.
 - **Yes:** Refer to (B1xx) Service processor firmware reference codes.
15. In the Integrated Virtualization Manager Navigation bar, select **Manage Serviceable Events** (under Service Management).
16. In the Serviceable Event Selection Criteria field, select the criteria for the serviceable events that you want to view, and click **Apply**. The Serviceable Events appear in the table below. The list shows all serviceable events that match your selection criteria. You can use the Tasks options to perform actions on the serviceable events.
17. Choose from the following options:
 - To view properties, continue with step 18.
 - To view associated FRUs, continue with step 19 on page 221.
 - To close a serviceable event, continue with step 20 on page 221.
 - To view additional details for a serviceable event, continue with step 21 on page 221.
18. To view properties for a serviceable event, select the serviceable event that you want to view properties for and select **Properties**. The Serviceable Event Comments window opens.

19. To view associated field replaceable units (FRUs), select the serviceable event that you want to view FRUs for, and select **View associated FRUs**. The Serviceable Event window opens.
20. To close a serviceable event, select one or more of the serviceable events that you want to close, and select **Close event**. The Serviceable Event Comments window opens.
 - a. Enter comments if necessary, and click **Close Events**.
 - b. On the Close Serviceable Event dialog, click Yes to close the serviceable event.
21. If you have SRUser role or DEUser role, you can view additional details for a serviceable event. Select the serviceable event that you want to view additional details for and select **View additional details**. The Serviceable Event Comments window opens listing additional service objects, each of which has a **Properties** task.
22. If you have not determined or resolved the problem, choose from the following options:
 - If you are having a problem with an AIX system or logical partition, continue with “AIX problem analysis.”
 - If you are having a problem with a Linux system or logical partition, continue with “Linux problem analysis” on page 232.

AIX problem analysis

Use this procedure to perform AIX problem analysis.

If you experience a problem with your AIX server or logical partition, you should attempt to gather more information about the problem to either solve it, or to help your next level of support or your hardware service provider to solve it more quickly and accurately.

Keep the following in mind while troubleshooting AIX server problems :

- Has there been an external power outage or momentary power loss?
- Has the hardware configuration changed?
- Has server software been added?
- Have any new programs or program updates been installed recently?

Check the following connections:

- Verify that the power cord is plugged in.
- Verify that all your cables are attached securely.

Has your server ever been configured with one or more logical partitions?

- **No:** Go to The server *has never been* partitioned and there is no HMC or Integrated Virtualization Manager.
- **Yes:** Go to The server *has been* partitioned and there is an HMC or an Integrated Virtualization Manager.

The server *has never been* partitioned and there is no HMC or Integrated Virtualization Manager

1. Is the server turned on, or can you turn on your server?
 - **No:** Go to step 2.
 - **Yes:** Ensure that the server is turned on and then go to step 4 on page 222.
2. Perform the following steps to verify that the server is receiving power:
 - a. If your server is protected by an emergency power off (EPO) circuit, check that the EPO switch is not activated.
 - b. If you have an uninterruptible power supply, verify that the cables are correctly connected to the server, and that it is functioning correctly.
 - c. When a good power source is connected to the server, one of the following occurs:

- If you have a control panel, the Function/Data display on the control (operator) panel is illuminated.
 - If you do not have a control panel, the Bulk Power Controller system lights are illuminated.
3. Is the control (operator) panel illuminated?
- **Yes:** Start the server by either pressing the power button on the control (operator) panel, and then go to step 4.
- Note:** If the server stops with a reference code appearing in the Function/Data display on the control (operator) panel, record the reference code and any related information, and go to “Reference codes list for customers” on page 263. **This ends the procedure.**
- **No:** There is a power problem. Verify that the power source to the server is functioning correctly (for example, the wall outlet is functioning correctly and the power cord is not damaged). If you cannot find a problem with the power source, contact your next level of support or your hardware service provider. **This ends the procedure.**
4. Is the control (operator) panel blank?
- **Yes:** Go to step 9.
 - **No:** Continue with the next step.
5. Is the Attention light on the control (operator) panel illuminated?
- **Yes:** Go to step 9.
 - **No:** Continue with the next step.
6. Are any additional messages related to this problem displayed on the system console or sent to you in e-mail from the operating system?
- **Yes:** Continue with the next step.
 - **No:** Contact your next level of support or your hardware service provider.
7. Record any additional message information that is available from the control (operator) panel, attached displays, or e-mail from the operating system.
8. If the additional message information contains recovery instructions, follow these instructions.
- Did this solve the problem?
- **Yes: This ends the procedure.**
 - **No:** Continue with the next step.
9. Is the operating system functioning?
- **Yes:** Continue with the next step.
 - **No:** Perform the following steps:
 - a. Obtain a list of error and event log entries from the ASMI’s Error/Event Logs. For details, see the Displaying error and event logs topic.
 - b. Continue with step 11 on page 223.
10. Record any SRN information that is displayed or available through e-mail.
- Note:** If you have not found an SRN, it is possible to display an SRN using the operating system. Perform the following to display previous diagnostic results from online diagnostics in concurrent mode:
- a. Log in to the AIX operating system as root user, or use CE login. If you need help, contact the system administrator.
 - b. Enter the diag command to load the diagnostic controller, and display the online diagnostic menus.
 - c. At the **Function selection** menu, select **Task selection**.
 - d. From the Task selection list menu, select **Display previous diagnostic results**.
 - e. From the Previous diagnostic results menu, select **Display diagnostic log summary**.

A Display diagnostic log will be shown with a time ordered table of events from the error log. Look in the T column for the most recent entry that has an S entry. Press Enter to select the row in the table and then select **Commit**. The details of this entry from the table will be displayed; look for the SRN entry shown near the end of the entry and record the information shown.

11. Record all other reference codes (if any are displayed) that you are receiving on the control (operator) panel. See “Collecting reference codes and system information” on page 260 for details.
12. Go to the “Reference codes list for customers” on page 263.

The server *has been* partitioned and there is an HMC or an Integrated Virtualization Manager.

If you have an HMC, it must be attached and functioning correctly.

1. Choose from the following options:
 - If you have an HMC, ensure you performed the steps in “Beginning problem analysis” on page 219. Then return here if you are directed to do so.
 - If you are using an Integrated Virtualization Manager, continue with the next step.
2. Can you start the server and at least one logical partition on your server?
 - **No:** Go to step 3.
 - **Yes:** Go to step 5.
3. Perform the following steps to verify that the server is receiving power:
 - a. If your server is protected by an emergency power off (EPO) circuit, check that the EPO switch is not activated.
 - b. If you have an uninterruptible power supply, verify that the cables are correctly connected to the server, and that it is functioning correctly.
 - c. When a good power source is connected to the server, one of the following occurs:
 - If you have a control panel, the Function/Data display on the control (operator) panel is illuminated.
 - If you do not have a control panel, the Bulk Power Controller system lights are illuminated.
4. Is the control (operator) panel or Bulk Power Controller illuminated?
 - **No:** There is a power problem. Verify that the power source to the server is functioning correctly (for example, the wall outlet is functioning correctly and the power cord is not damaged). If you cannot find a problem with the power source, contact your next level of support or your hardware service provider. **This ends the procedure.**
 - **Yes:** Start the server.

Note:

If the server stops with a reference code appearing in the Function/Data display on the control (operator) panel, or on the HMC, or on the Integrated Virtualization Manager, record the reference code and any related information, and go to the “Reference codes list for customers” on page 263 for further information. **This ends the procedure.**

5. Is the server’s control (operator) panel, the HMC, or Integrated Virtualization Manager displaying function 11?

Note: If you are using the control panel, use the increment or decrement buttons to cycle through the functions to determine if function 11 exists. You can alternate between the function number and the data by pressing Enter. For details, see “Collecting reference codes and system information” on page 260.

- **Yes:** Go to step 9 on page 224.
 - **No:** Continue with the next step.
6. Is the system attention light on?
 - **Yes:** Go to step 9 on page 224.

- **No:** Continue with the next step.
7. Did you receive a message related to this problem either through the mail function or shown on the HMC or Integrated Virtualization Manager?
 - **Yes:** Continue with the next step.
 - **No:** Contact your next level of support or your hardware service provider.
 8. Record the additional message information on the problem reporting form. For details, see “Using the problem reporting forms” on page 443. Then follow the recovery instructions on the Additional Message Information display. Did this solve the problem?
 - **Yes: This ends the procedure.**
 - **No:** Continue with the next step.
 9. Perform the following:
 - a. Record all the reference codes that you are receiving on the control (operator) panel, the HMC, or the Integrated Virtualization Manager. For details, see “Collecting reference codes and system information” on page 260.
 - b. Go to the “Reference codes list for customers” on page 263.

IBM i5/OS problem analysis

Use this procedure to perform i5/OS problem analysis.

If you experience a problem with your i5/OS system or logical partition, gather more information about the problem to either solve it, or to help your next level of support or your hardware service provider to solve it more quickly and accurately.

This procedure refers to the i5/OS control language (CL) commands, which provide a flexible means of entering commands on the i5/OS logical partition or system. You can use CL commands to control most of the i5/OS functions by entering them from either the character-based interface or iSeries Navigator. While the CL commands might be unfamiliar at first, they follow a consistent syntax, and i5/OS includes many features to help you use them successfully. The CL topic includes a complete CL reference and a CL finder to look up specific CL commands.

Keep the following in mind while troubleshooting i5/OS problems:

- Has an external power outage or momentary power loss occurred?
- Has the hardware configuration changed?
- Has system software been added?
- Have any new programs or program updates (including PTFs) been installed recently?

To make sure that your IBM software has been correctly installed, use the Check Product Option (CHKPRDOPT) command.

- Have any system values changed?
- Has any system tuning been done?

After reviewing these considerations, follow these steps:

1. If you have an HMC, ensure you performed the steps in “Beginning problem analysis” on page 219. Then return here if you are directed to do so.

Note: For details on accessing a 5250 console session on the HMC, see Managing the HMC 5250 console.

2. Can you start your system?
 - **Yes:** Continue with the next step.
 - **No:** Go to “Recovering from a system power problem” on page 228.

3. Are you troubleshooting a problem related to the iSeries integrated xSeries® or blade server within an iSCSI environment?
 - **No:** Continue with the next step.
 - **Yes:** Refer to the System i integration with BladeCenter® and System x® Web site at <http://www-03.ibm.com/systems/i/bladecenter/>
4. Is the system control panel displaying function 11 (use the increment or decrement buttons to cycle through the functions to determine if function 11 exists. Press Enter to alternate between function and data).
 - **Yes:** Go to step 23 on page 227.
 - **No:** Continue with the next step.
5. Is the system attention light on?
 - **Yes:** Go to step 23 on page 227.
 - **No:** Continue with the next step.
6. Choose from the following options:
 - If you are using a twinaxial console, continue with the next step.
 - If you are using an Operations Console, refer to Troubleshooting Operations Console connections.
 - If you are using a Thin Console, refer to Troubleshooting the Thin Console.
7. Does the console show a Main Storage Dump Manager display?
 - **Yes:** Go to Copying a dump.
 - **No:** Continue with the next step.
8. Does the console that was in use when the problem occurred (or any console) appear to be operational?

Note: The console is operational if a sign-on display or a command line is present. If another console is operational, use it to resolve the problem.

 - **Yes:** Continue with the next step.
 - **No:** Choose from the following options:
 - If your console does not show a sign-on display or a menu with a command line, go to “Recovering when the console does not show a sign-on display or a menu with a command line” on page 231.
 - For all other workstations, go to “Recovering from a workstation failure” on page 229.
9. Is a message related to this problem shown on the console?
 - **Yes:** Continue with the next step.
 - **No:** Go to step 15 on page 226.
10. Is this a system operator message?

Note: It is a system operator message if the display indicates that the message is in the QSYSOPR message queue. Critical messages can be found in the QSYSMSG message queue. For more information, refer to Create message queue QSYSMSG for severe messages.

 - **Yes:** Continue with the next step.
 - **No:** Go to step 12.
11. Is the system operator message highlighted, or does it have an asterisk (*) by it?
 - **Yes:** Go to step 22 on page 227.
 - **No:** Go to step 17 on page 226.
12. Move the cursor to the message line and press F1 (Help). Does the Additional Message Information display appear?
 - **Yes:** Continue with the next step.
 - **No:** Go to step 15 on page 226.

13. Record the additional message information on the appropriate problem reporting form. For details, see "Using the problem reporting forms" on page 443.
14. Then follow the recovery instructions on the Additional Message Information display. Did this solve the problem?
 - **Yes: This ends the procedure.**
 - **No:** Continue with the next step.
15. To display system operator messages, type `dspmsg qsysopr` on any command line and press Enter. Did you find a message that is highlighted or has an asterisk (*) by it?
 - **No:** Continue with the next step.

Note: The message monitor in iSeries Navigator can also inform you when a problem has developed. For details, see Scenario: Message monitor.

- **Yes:** Go to step 22 on page 227.
16. Did you find a message with a date or time that is at or near the time the problem occurred?

Note: Move the cursor to the message line and press F1 (Help) to determine the time a message occurred. If the problem is shown to affect only one console, you might be able to use information from the JOB menu to diagnose and solve the problem. To find this menu, type `G0 JOB` and press Enter on any command line.

- **Yes:** Continue with the next step.
 - **No:** Go to step 19.
17. Perform the following steps:
 - a. Move the cursor to the message line and press F1 (Help) to display additional information about the message.
 - b. Record the additional message information on the appropriate problem reporting form. For details, see "Using the problem reporting forms" on page 443.
 - c. Follow any recovery instructions that are shown.

Did this solve the problem?

- **Yes: This ends the procedure.**
 - **No:** Continue with the next step.
18. Did the message information indicate to look for additional messages in the system operator message queue (QSYSOPR)?
 - **No:** Continue with the next step.
 - **Yes:** Press F12 (Cancel) to return to the list of messages and look for other related messages. Then return to step 15.
 19. Do you know which input/output device is causing the problem?
 - **No:** Continue with the next step.
 - **Yes:** Continue with step 21 on page 227.
 20. If you do not know which input/output device is causing the problem, describe the problems that you have observed by performing the following steps:
 - a. Type `G0 USERHELP` on any command line and press Enter.
 - b. Select option 10 (Save information to help resolve a problem).
 - c. Type a brief description of the problem and press Enter. If you specify the default Y in the **Enter notes about problem** field, you can enter more text to describe your problem.

Note: To describe your problem in greater detail, see Use the Analyze Problem (ANZPRB) command. This command also can run a test to further isolate the problem.

- d. Report the problem to your hardware service provider. For details, see "Contacting IBM service and support" on page 447.

21. Perform the following steps:
 - a. Type ANZPRB on the command line and press Enter. For details, see Use the Analyze Problem (ANZPRB) command.
 - b. Report the problem. For details, see “Contacting IBM service and support” on page 447. **This ends the procedure.**
22. Perform the following steps:
 - a. Move the cursor to the message line and press F1 (Help) to display additional information about the message.
 - b. Press F14, or use the Work with Problem (WRKPRB) command. For details, see Use the Work with Problems (WRKPRB) command.
 - c. If this does not solve the problem, see the “Symptom and recovery actions.”
23. Choose from the following options:
 - If there are reference codes appearing on the control panel or the HMC, record them. For details, see “Collecting reference codes and system information” on page 260. Then go to the “Reference codes list for customers” on page 263 to see if there are additional details available for the code you received.
 - If there are no reference codes appearing on the control panel or the HMC, there should be a serviceable event indicated by a message in the problem log. Use the WRKPRB command. For details, see Use the Work with Problems (WRKPRB) command.

Symptom and recovery actions

Use this procedure to determine symptoms and find recovery actions for i5/OS.

1. Were you directed here from the problem analysis procedure?
 - **Yes:** Continue with the next step.
 - **No:** Go to “IBM i5/OS problem analysis” on page 224.
2. To find the symptom for the problem, look in the Symptom column in the following table, starting at the top and moving down the list. Then perform the procedure listed in the Recovery procedure column.

Table 4. Problem analysis symptom and recovery list

Symptom	Recovery procedure
You cannot turn on the system.	See “Recovering from a system power problem” on page 228.
The system attention light is on, or a reference code is displayed on the control panel.	See the “Reference codes list for customers” on page 263.
The Operations Console remote control panel feature is not working correctly.	See “Recovering when the remote control panel interface of Operations Console is not working correctly” on page 228.
A button or light on the control panel is not working correctly.	Turn on the system again. If the control panel buttons or lights still are not working correctly, contact your next level of support or your hardware service provider.
You cannot perform an initial program load (IPL) or you suspect an operating system failure.	See “Recovering from IPL or system failures” on page 229.
Your workstation or device (such as display or printer) is not working.	See “Recovering from a workstation failure” on page 229.
You are having a problem with a tape or CD drive.	See “Recovering from a tape or CD drive problem” on page 230.
You cannot communicate with another device or computer.	See “Recovering from a communications problem” on page 230.

Table 4. Problem analysis symptom and recovery list (continued)

Symptom	Recovery procedure
Your system seems to be in a hang or loop condition.	See "Recovering from system hang or loop condition" on page 231.
You are having an intermittent problem.	See "Recovering from an intermittent problem" on page 231.
You are having data compression problems and receive message CPPEA02 along with reference code 6xxx 7051 (Compressed device and compression input/output adapter (IOA) are not compatible).	Go to "Recovering from SRC 6xxx 7051" in the Working with Disk Compression chapter in the Backup and Recovery guide (about 4 MB).
You are having data compression problems and receive message CPPEA03 along with reference code 6xxx 7052 (Data compression warning).	Go to "Recovering from SRC 6xxx 7052" in the Working with Disk Compression chapter in the Backup and Recovery guide (about 4 MB).
No symptom matches those in the table.	Contact your next level of support. For details, see "Contacting IBM service and support" on page 447.

Recovering from a system power problem

Use this procedure to help resolve power problems for i5/OS.

1. Make sure that the power supplied to the system is adequate. If your system units are protected by an emergency power off (EPO) circuit, check that the EPO switch is not activated.
2. Verify that your system power cables are correctly connected to the electrical outlet. When power is available, the Function/Data display on the control panel is lit.
3. If you have an uninterruptible power supply, verify that the cables are correctly connected to the system, and that it is functioning.
4. Make sure all system units are started.
5. Start the system again. Is a reference code displayed on the control panel?
 - **Yes:** Go to the "Reference codes list for customers" on page 263.
 - **No:** Contact your next level of support or your hardware service provider.

Recovering when the remote control panel interface of Operations Console is not working correctly

Use this procedure to help resolve problems when the remote control interface of Operations Console is not working correctly for i5/OS.

For additional information on using Operations Console, see the Operations Console topic.

1. Are you able to change modes or select system functions using the remote control panel feature?
 - **Yes:** Continue with the next step.
 - **No:** Make sure the Operations Console cable is attached correctly. Using the Operations Console display, disconnect and then reconnect the server connection. If the same failure occurs, contact your next level of support or your hardware service provider.
2. Are the remote control panel functions (Function/Data, Mode and Power) correctly displayed?
 - **Yes:** Use the remote control panel to start an IPL (initial program load) and continue with the next step.
 - **No:** Contact your next level of support or your hardware service provider.
3. Was the IPL successfully started?
 - **Yes:** Continue the IPL process.
 - **No:** Contact your next level of support or your hardware service provider.

Recovering from IPL or system failures

Use this procedure to help recover from IPL or system failures for i5/OS.

Verify the following:

- The device from which you performed the IPL (initial program load) is started.
- The tape and CD are inserted correctly.
- The sign-on user ID and password are correct.
- The system is set to the correct mode (Manual, Normal, Auto, or Secure).
- If this is a timed IPL, the system value for date/time and control panel mode is set correctly.
- If this is a remote IPL, the telephone, modem, control panel mode, and QRMTIPL system value are set up correctly.

Perform the following steps to recover from an IPL or system failures:


1. Follow these steps to perform an IPL from the control panel or Operations Console Remote Control panel:
 - a. Set the system to the Manual mode.
 - b. Choose from the following:
 - If the system is turned on, select function 03 and press Enter to start an IPL.
 - If the system is shut off, ensure that the control panel is in either Normal or Manual mode and press the power-on button.
2. Choose from the following options:
 - If you see the Sign On display, sign onto the system, and continue with step 3.
 - If you do not see the Sign On display, do you have a new reference code?
 - **Yes:** Record the code and go to the “Reference codes list for customers” on page 263.
 - **No:** Contact your next level of support or your hardware service provider. For details, see “Contacting IBM service and support” on page 447.
3. On the IPL Options display, specify Yes for the following parameters:
 - Define or change the system at IPL
 - Clear output queues
 - Clear job queues
 - Clear incomplete job logs
4. Change the system value for QMCHPOOL to a smaller value.
5. Make sure the system value for QCTLSBSD has the correct spelling, or assign an alternative controlling subsystem.
6. Change the system value for QPWRDWNLMT to a larger value.
7. Continue the IPL process.

If the same failure occurs, set the system to the Normal mode, and then contact your next level of support or your hardware service provider.

Recovering from a workstation failure

Use this procedure to help recover from a workstation failure for i5/OS.

1. Make sure all workstations and devices (such as displays or printers) are turned on.
2. Ensure that the cable from the console to the server is attached correctly.
3. Make sure that the console has been correctly configured.
4. Make sure that all workstation cables are attached correctly, and that all workstations are set to the correct address. For information about the workstation address, see the following:

- If you are using an HMC or Operations Console, see “Determining the primary or alternate console” on page 427.
 - If you are using other workstations, see the Local Device Configuration book  .
5. Ensure the following conditions exist:
 - Recently attached workstations have been correctly configured to the system.
 - Workstation addresses are unique, if applicable.
 - Workstations are turned off, if applicable.
 6. Check all workstation printers for mechanical problems, such as paper jams, ribbon failure, and so on.
 7. If you are using an iSeries Operations Console, vary off the failing workstation controller if another workstation is operational, and then vary it on again. Follow these steps to vary on or vary off the workstation controller:
 - a. Type WRKCFGSTS *CTL on any command line. The Work with Configuration Status display is shown.
 - b. Specify 1 (Vary-on) or 2 (Vary-off) in the Opt column next to your workstation controller and press Enter.
 - c. End all active jobs before varying off the workstation controller using the Work with Active Jobs (WRKACTJOB) command.
 8. Try the operation again.

If you are still having the same problem, contact your next level of support or your hardware service provider.

Recovering from a tape or CD drive problem

Use this procedure to help resolve tape or CD drive problems for i5/OS.

Verify the following:

- All tape or CD drives are started and in a Ready (enabled) condition.
- Cables between the system and the tape or CD drive are correctly connected, if applicable.
- Tape density and tape bits per inch (BPI) match.
- The tape path is clean.
- The CD is clean, the format is supported, and the CD is inserted correctly with the label side showing.

Do all the tape or CDs still fail to read or write?

- **Yes:** Contact your next level of support or your hardware service provider.
- **No:** Replace the tape or CD and try the operation again. If the same failure occurs, contact your next level of support or your hardware service provider.

Recovering from a communications problem

Use this procedure to help resolve problems with communications for IBM i5/OS.

Verify the following:

1. Make sure that all communications equipment, such as modems or transceivers, are started.
2. Make sure all communication cables are correctly connected.
3. Make sure the remote system is ready to receive communications.
4. Verify that the network equipment (or provider) is functional. This includes telephone service (for example, verify the status of communication lines).
5. Verify that the configuration is correctly specified for the failing communications or LAN facility.
6. If you still have the same problem, contact your next level of support or your hardware service provider.

Recovering from system hang or loop condition

Use this procedure to help resolve a system hang or loop condition for i5/OS.

1. Perform a main storage dump to gather data on the current state of the system during the hang or loop condition. Refer to “Performing dumps” on page 416.

This information is critical for problem solving. Valuable diagnostic information will be lost if you do not collect the storage dump information before you try to perform an IPL.

2. Contact your next level of support or your hardware service provider after performing the main storage dump.

Recovering from an intermittent problem

Use this procedure to help resolve intermittent problems for i5/OS.

Perform the following steps:

1. Enter the Analyze Problem (ANZPRB) command on any command line.
2. Select option 1 (This server or attached device) on the Select Type of System display.
3. Select option 3 (Hardware problem) on the Analyze problem display.
4. Select option 1 (Yes) on the Problem Frequency display to get an intermittent checklist and follow the instructions.
5. If you still have the same problem, contact your next level of support or your hardware service provider.

Recovering when the console does not show a sign-on display or a menu with a command line

Use this procedure to recover when the console does not show a sign-on display or a menu with a command line for i5/OS.

Perform the following steps:

1. Locate the workstation that is used as the primary console. See “Determining the primary or alternate console” on page 427.
2. Make sure the workstation cables are attached correctly and are set to the correct address.
3. Can you sign on to an alternative console?
 - **Yes:** Continue with the next step.
 - **No:** Go to step 5.
4. If you can sign on to an alternative console, do the following:
 - a. Make sure the primary console controller (for example, CTL01) and device description (for example, DSP01) have been created or restored. To check the device description, use the command `WRKCFGSTS *CTL`.
 - b. If descriptions exist, check the system operator message to determine why the primary console failed.
 - c. Take corrective actions indicated in the message.
 - d. If you still cannot solve the problem, set the system to the Normal mode and call your hardware service provider.
5. If you cannot sign on to an alternative console, perform a manual IPL by following these steps:
 - a. Set the system to Manual mode.
 - b. Select function 3 and press Enter. The IPL Option display is shown.
6. Were you able to get to the IPL Option display?
 - **No:** Contact your next level of support or your hardware service provider.
 - **Yes:** Continue with the next step.
7. To access the Configuration Commands menu, perform the following steps on the IPL Options display:

- a. Specify Y (Yes) in the Define or change system at IPL field
 - b. Specify N (No) in the Set major system option field and press Enter.
8. To see the controller description for the console, select option 2 (Controller description commands).
 - a. Verify that the controller was created correctly (for example, CTL01).
 - b. If the name has been changed, see “Find the primary console when the system is operational” on page 427.
9. To see the device description for the console, select option 3 (Device description commands).
 - a. Verify that the device was created correctly (for example, DSP01).
 - b. If the name has been changed, see “Find the primary console when the system is operational” on page 427.

Linux problem analysis

Use this procedure to perform Linux problem analysis.

If you experience a problem with your Linux system or logical partition, attempt to gather more information about the problem to either solve it, or to help your next level of support or your hardware service provider to solve it more quickly and accurately.

Note: While troubleshooting Linux, you might need to have available service tools. For details, see “Obtaining service and productivity tools for Linux” on page 207.

Keep the following in mind while troubleshooting Linux problems:

- Has there been an external power outage or momentary power loss?
- Has the hardware configuration changed?
- Has system software been added?
- Have any new programs or program updates been installed recently?

Check the following connections:

- Verify that the power cord is plugged in.
- Verify that your cables are attached securely.

Has your server ever been configured with one or more logical partitions?

- **No:** Go to The server *has never been* partitioned and there is no HMC or Integrated Virtualization Manager.
- **Yes:** Go to The server *has been* partitioned and there is an HMC or Integrated Virtualization Manager.

The server *has never been* partitioned and there is no HMC or Integrated Virtualization Manager

1. Is the server turned on, or can you turn on your server?
 - **No:** Go to step 2.
 - **Yes:** Ensure that the server is turned on and then go to step 4 on page 233.
2. Perform the following steps to verify that the server is receiving power:
 - a. If your server is protected by an emergency power off (EPO) circuit, check that the EPO switch is not activated.
 - b. If you have an uninterruptible power supply, verify that the cables are correctly connected to the server, and that it is functioning correctly.
 - c. When a good power source is connected to the server, one of the following occurs:
 - If you have a control panel, the Function/Data display on the control (operator) panel is illuminated.
 - If you do not have a control panel, the Bulk Power Controller system lights are illuminated.

3. Is the control (operator) panel illuminated?
 - **Yes:** Start the server by pressing the power button on the control (operator) panel, and then go to step 4.

Note: If the server stops with a reference code appearing in the Function/Data display on the control (operator) panel, record the reference code and any related information, and go to “Reference codes list for customers” on page 263. **This ends the procedure.**

 - **No:** There is a power problem. Verify that the power source to the server is functioning correctly (for example, the wall outlet is functioning correctly and the power cord is not damaged). If you cannot find a problem with the power source, contact your next level of support or your hardware service provider. **This ends the procedure.**
4. Is the control (operator) panel displaying a reference code?
 - **Yes:** Continue with the next step.
 - **No:** Go to step 9.
5. Is the Attention light on the control (operator) panel illuminated?
 - **Yes:** Go to step 9.
 - **No:** Continue with the next step.
6. Are any additional messages (for example a device is not available or reporting errors) related to this problem displayed on the system console or sent to you in e-mail from the operating system?
 - **Yes:** Continue with the next step.
 - **No:** Contact your next level of support or your hardware service provider.
7. Record any additional message information that is available from the control (operator) panel, attached displays, or e-mail from the operating system.
8. If the additional message information contains recovery instructions, follow these instructions.

Did this solve the problem?

 - **Yes: This ends the procedure.**
 - **No:** Continue with the next step.
9. Is the operating system functioning?
 - **Yes:** Continue with the next step.
 - **No:** Perform the following steps:
 - a. Refer to the ASMI’s Error/Event Logs to obtain a list of error and event log entries. For details, see the Displaying error and event logs topic.
 - b. Continue with step 11.
10. Run the eServer stand-alone diagnostics in Problem Determination mode. For details, see “Running the eServer stand-alone diagnostics from CD-ROM” on page 408. Record any SRN information that is displayed or available through e-mail. When you run the eServer stand-alone diagnostics in Problem Determination mode, you are given the option to test the resources that the diagnostic programs find in your server. Be sure to check the list of available resources in your server to make sure that all resources that you know are installed are also available to be tested. If you find that a resource you know to be installed in your system is not available to be tested, record any information that is available about the missing resource, and check to ensure that the missing resource is installed correctly. If you cannot correct the problem with a missing resource, replace the missing resource (contact your service provider if necessary).
11. Record all other reference codes (if any are displayed) that you are receiving on the control (operator) panel. See “Collecting reference codes and system information” on page 260 for details.
12. Go to the “Reference codes list for customers” on page 263.

The server *has been* partitioned and there is an HMC or Integrated Virtualization Manager.

If you have an HMC, it must be attached and functioning correctly.

1. Choose from the following options:
 - If you have an HMC, ensure you performed the steps in “Beginning problem analysis” on page 219. Then return here if you are directed to do so.
 - If you are using an Integrated Virtualization Manager, continue with the next step.
2. Can you start the server and at least one logical partition on your server?
 - **No:** Go to step 3.
 - **Yes:** Go to step 5.
3. Perform the following steps to verify that the server is receiving power:
 - a. If your server is protected by an emergency power off (EPO) circuit, check that the EPO switch is not activated.
 - b. If you have an uninterruptible power supply, verify that the cables are correctly connected to the server, and that it is functioning correctly.
 - c. When a good power source is connected to the server, one of the following occurs:
 - If you have a control panel, the Function/Data display on the control (operator) panel is illuminated.
 - If you do not have a control panel, the Bulk Power Controller system lights are illuminated.
4. Is the control (operator) panel or Bulk Power Controller illuminated?
 - **No:** There is a power problem. Verify that the power source to the server is functioning correctly (for example, the wall outlet is functioning correctly and the power cord is not damaged). If you cannot find a problem with the power source, contact your next level of support or your hardware service provider. **This ends the procedure.**
 - **Yes:** Start the server.

Note:

If the server stops with a reference code appearing in the Function/Data display on the control (operator) panel, or on the HMC, or on the Integrated Virtualization Manager, record the reference code and any related information, and go to the “Reference codes list for customers” on page 263 for further information. **This ends the procedure.**

5. Is the server’s control (operator) panel, HMC, or Integrated Virtualization Manager displaying function 11?

Note: If you are using the control panel, use the increment or decrement buttons to cycle through the functions to determine if function 11 exists. You can alternate between the function number and the data by pressing Enter. For details, see “Collecting reference codes and system information” on page 260.

 - **Yes:** Go to step 10 on page 235.
 - **No:** Continue with the next step.
6. Is the system attention light on?
 - **Yes:** Go to step 10 on page 235.
 - **No:** Continue with the next step.
7. Did you receive a message related to this problem either through the mail function or shown on the HMC or Integrated Virtualization Manager?
 - **Yes:** Continue with the next step.
 - **No:** Contact your next level of support or your hardware service provider.
8. Record the additional message information on the problem reporting form. For details, see “Using the problem reporting forms” on page 443. Then follow the recovery instructions on the Additional Message Information display. Did this solve the problem?
 - **Yes:** **This ends the procedure.**
 - **No:** Continue with the next step.

9. Record any SRN information that is displayed or available through e-mail. If you do not have any SRN information, run the eServer stand-alone diagnostics in Problem Determination mode. For details, see "Running the eServer stand-alone diagnostics from CD-ROM" on page 408 and perform any repair actions.
10. Perform the following:
 - a. Record all the reference codes that you are receiving on the control (operator) panel, the HMC, or the Integrated Virtualization Manager. For details, see "Collecting reference codes and system information" on page 260.
 - b. Go to the "Reference codes list for customers" on page 263.

HMC problem analysis

Use this information to diagnose and repair problems that are related to the Hardware Management Console (HMC).

DANGER

When working on or around the system, observe the following precautions:

Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard:

- Connect power to this unit only with the IBM provided power cord. Do not use the IBM provided power cord for any other product.
- Do not open or service any power supply assembly.
- Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.
- The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords.
- Connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate.
- Connect any equipment that will be attached to this product to properly wired outlets.
- When possible, use one hand only to connect or disconnect signal cables.
- Never turn on any equipment when there is evidence of fire, water, or structural damage.
- Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.
- Connect and disconnect cables as described in the following procedures when installing, moving, or opening covers on this product or attached devices.

To Disconnect:

1. Turn off everything (unless instructed otherwise).
2. Remove the power cords from the outlets.
3. Remove the signal cables from the connectors.
4. Remove all cables from the devices


To Connect:

1. Turn off everything (unless instructed otherwise).
2. Attach all cables to the devices.
3. Attach the signal cables to the connectors.
4. Attach the power cords to the outlets.
5. Turn on the devices.

(D005)

If you were directed here from the Beginning problem analysis procedure because your HMC is not functioning correctly, continue with the "Entry point for HMC problem determination" on page 236.

To perform other maintenance tasks on your HMC, refer to the following procedures:

- For general maintenance information on the base personal computer that is used to build the HMC, see “HMC diagnostics overview” on page 248.
- For instructions to replace an HMC, see Replacing an HMC.
- For HMC parts information, refer to the following:
 - Hardware Management Console (HMC) parts . Because the personal computer that is used for your HMC can be serviced by the customer, you are the service provider for your HMC.
 - To find links to the appropriate personal computer hardware maintenance information, see “Equivalent maintenance information for the HMC’s personal computer hardware” on page 250.
- For removing and replacing HMC parts, see “Removing and replacing parts on the HMC” on page 253.
- For backing up critical disk drive information on the HMC, refer to the Backing up critical HMC data topic.
- For restoring disk drive information on the HMC, refer to Reinstalling the HMC machine code .
- For checking modem settings, refer to the Cabling the HMC topic.
- For troubleshooting setting up an HMC or installing the remote client, see Troubleshooting HMC setup.

Entry point for HMC problem determination

Find the symptom you are having in the Symptom column of the following table. Then perform the action described in the Action column.

Symptom	Action
Operator reported that the HMC did not start, but no other problems were reported.	Go to “Beginning HMC problem determination” on page 237.
Operator reported “Communication not active” on the HMC.	Go to “Testing the HMC’s Ethernet adapter” on page 242.
Operator reported communication problems with a remotely connected HMC or a managed system.	Go to “Testing the modem connection to the managed system” on page 239.
Power problems	Go to “Testing for a power problem” on page 238.
HMC boot problems	Go to “Beginning HMC problem determination” on page 237.
Display problem	Go to “Testing the HMC’s display” on page 246.
DVD-RAM drive problem	Go to “Testing the HMC’s DVD-RAM” on page 243.
Diskette drive problem	Go to “Testing the HMC’s diskette drive” on page 245.
Ethernet LAN problem	Go to “Testing the HMC’s Ethernet adapter” on page 242.
A problem with any of the following: <ul style="list-style-type: none"> • display • diskette drive • DVD-RAM Drive • disk drive • Ethernet LAN 	Go to “Performing system unit testing using PC-Doctor” on page 239.
Eight character error code beginning with <i>HMC</i> was received when using the HMC graphical user interface.	Go to the “HMC error codes” on page 271.

Symptom	Action
HMC does not communicate through the modem.	Go to "Testing the HMC's modem connection" on page 240.
PC-Doctor diagnostic tests detected an error.	For PC hardware maintenance manuals to help isolate the problem to a failing part, refer to "Equivalent maintenance information for the HMC's personal computer hardware" on page 250.
Problems understanding the usage of the HMC.	Go to Managing your server using the Hardware Management Console.
All other problems (for example: HMC GUI is unresponsive, parity errors, power, POST codes, blank display, mouse, or keyboard).	Go to "Beginning HMC problem determination."
Symptoms not in this list.	Go to "Beginning HMC problem determination."

Beginning HMC problem determination

Use this procedure to determine if there is a problem with the HMC hardware. This procedure might direct you to procedures in various sections of this information or to personal computer maintenance information.

Step 1. HMC problem determination:

1. If the HMC is running, shut down the console by exiting the graphical user interface, the PC should turn off the power automatically. If the PC cannot turn off the power, then turn the power switch off.
2. Turn on the HMC power.
3. Watch the console and allow enough time for the system to complete the POST and load the HMC machine code.
4. Watch and listen for the following failing symptoms during power-on:
 - POST error condition.
 - A series of beeps that indicate an error condition.
 - The HMC login screen and user interface fails to start.
 - A reference code or any other error information is displayed.
5. Do you have any of the failing symptoms during power on?
 - **No:** Continue with step 6.
 - **Yes:** Go to the "General Checkout" section of the hardware maintenance manual for your machine type. For details, see "Equivalent maintenance information for the HMC's personal computer hardware" on page 250.
6. Perform system unit testing using PC-Doctor. For details, see "Performing system unit testing using PC-Doctor" on page 239.
7. Does the PC-Doctor diagnostics diskette start and allow tests to be run on the PC system unit?
 - **No:** Go to "Testing for a power problem" on page 238.
 - **Yes:** Go to "Step 2. HMC problem determination."

Step 2. HMC problem determination:

1. Perform system unit testing using PC-Doctor. For details, see "Performing system unit testing using PC-Doctor" on page 239. Select **System Unit** → **Run All Selected**.
2. Did the system unit tests detect errors?
 - **No:** Go to "Step 3. HMC problem determination" on page 238.
 - **Yes:** Continue with step 3 on page 238.

3. Use the PC-Doctor diagnostics and the maintenance procedures for the type of PC that you are working on to isolate the failure and exchange customer replaceable units (CRUs). Refer to the publications listed in the “Equivalent maintenance information for the HMC’s personal computer hardware” on page 250.
4. When the problem is repaired, or if the problem cannot be isolated, continue with “Step 4. HMC problem determination.”

Step 3. HMC problem determination:

Attention: This step requires HMC support assistance. Contact HMC support before continuing.

1. If you are directed to reload the HMC from the recovery DVD and then reload the backup profile and configuration data, see Recovering the HMC.
2. After reloading the machine code from the recovery DVD, does the HMC start correctly?
 - **No:** Contact your next level of support.
 - **Yes: This ends the procedure.**

Step 4. HMC problem determination:

Note: If you reach this step and you have not been able to isolate a failure, contact your next level of support for assistance.

1. Reinstall all CRUs that did not fix the problem.
2. You must have performed a repair action to continue. If you have not already done so, verify the repair. For instructions, see “Performing system unit testing using PC-Doctor” on page 239.
3. Did the system unit tests run without errors?
 - **No:** To troubleshoot the error, return to “Performing system unit testing using PC-Doctor” on page 239. Then return here and continue with step 4.
 - **Yes:** Continue with step 4.
4. Does the HMC communicate with all connected managed systems?
 - **No:** Go to “Testing the modem connection to the managed system” on page 239.
 - **Yes:** Did you exchange the system board or the system board battery?
 - **No: This ends the procedure.**
 - **Yes:** Recover the HMC. For details, see Recovering the HMC. **This ends the procedure.**

Testing the HMC

Use these procedures when you are directed to them from the HMC problem analysis procedure to test the HMC. If a failure is detected, you will be instructed to fix the failing part and then verify the repair.

Testing for a power problem:

To troubleshoot a power problem on the PC, refer to the service documentation for the PC on which your HMC is based. For PC hardware maintenance manuals to help isolate the problem to a failing part, refer to the publications listed in “Equivalent maintenance information for the HMC’s personal computer hardware” on page 250.

Performing diagnostic procedures:

You should have been directed here to test a specific part of the HMC. For the following problem areas, see “Performing system unit testing using PC-Doctor” on page 239:

- Display
- Keyboard
- Mouse

- Floppy Drive
- DVD-RAM
- DASD (disk drive)
- Memory
- Power
- Run All Selected
- SCSI
- System Port/Modem
- 16/4 Port Serial
- Ethernet

To access the HMC diagnostic information, follow the procedures in “HMC diagnostics overview” on page 248.

Performing system unit testing using PC-Doctor:

This section provides information to help you use the PC-Doctor diagnostics. For information on running PC-Doctor, go to “HMC diagnostics overview” on page 248.

Note: Performing procedures other than those specified in the following steps might cause errors.

1. Start the PC-Doctor diagnostics.
2. From the diagnostic selection display, select either **Diagnostics** or **Interactive Tests** for a list of devices to test:
 - Devices that require manual intervention (keyboard, video, mouse, diskette, optical drive) might be selected from the interactive tests task bar.
 - Devices that do not require manual intervention (processor, system board, I/O ports, fixed disks, memory) and predefined test sequences (Run Normal/Quick Test) can be selected from the diagnostic task bar.
3. Select the task containing the device or devices or test or tests and follow the instructions. If you were instructed to **Run All Selected**, continue with that selection.
4. If the diagnostics report a failure on the PC hardware, refer to the service documentation for the PC on which your HMC is based. For PC hardware maintenance manuals to help isolate the problem to a failing part, refer to the publications listed in “Equivalent maintenance information for the HMC’s personal computer hardware” on page 250.
5. If the diagnostics do not report a failure, the HMC PC hardware is functioning correctly. If you still have a problem, go to “Beginning HMC problem determination” on page 237.

Testing the modem connection to the managed system:

Use this procedure to test the modem connection to the PC for the HMC.


1. Can the HMC be used to communicate through the modem?
 - **No:** Go to step 2.
 - **Yes: This ends the procedure.**
2. Is a device other than a modem attached to system port 2 on the HMC?

Note: If the HMC is a rack-mounted model, answer no to this question.

- **No:** Go to “Testing the HMC’s modem connection” on page 240.
- **Yes:** Go to step 3 on page 240.

3. System port 2 of the HMC is reserved for external modem use only. Move the serial cable from serial port 2 of the HMC to another HMC system port. Connect the modem to system port 2 and go to step 1 on page 239.

Note: If the HMC is a rack-mounted model, an internal modem is installed to handle the connection of the HMC to the telephone line. If a redundant telephone connection is required, connect an external modem to the system port on the rear of the HMC. If needed, go to the MultiTech MultiModem^{II} installation guide for modem installation instructions. If you do not have access to a hardcopy version

of the MultiTech MultiModem^{II} documentation, go to the MultiTech  Web site at <http://www.multitech.com/documents/families/multimodemII/manuals.asp>.

Testing the HMC's modem connection:

Use this procedure to test the modem connection to the PC for the HMC.

1. Verify that the modem and the telephone line are functioning correctly by performing the following steps:
 - a. On the HMC console, open the Service Agent application.
 - b. Select **Test Tools**.
 - c. Initiate a Test PMR.
 - d. Monitor the call log to verify that the call is completed successfully. If the call is completed successfully, the modem is functioning correctly.
2. Is the installed modem currently functioning on the HMC?
 - **No:** Go to step 3.
 - **Yes:** The problem is not in the modem. **This ends the procedure.**
3. Are the HMC configurations, relating to the modem operation, correct?
 - **No:** Correct the HMC configuration arguments. Return to step 1.
 - **Yes:** Continue with step 4.
4. Is the modem powered on? (Are any indicators lit?)
 - **No:** Ensure the modem is powered on. For details, see 1. After power on verification is completed, continue with step 5.
 - **Yes:** Go to step 5.
5. Is the serial cable between the serial (COM) port connector of the HMC and the modem attached?
 - **No:** Attach the serial cable between the serial (COM) port connector of the HMC and the modem.
 - **Yes:** Load the PC-Doctor diagnostics.
 - If you are working on a desktop model HMC, load the PC-Doctor from diskette or CD.
 - If you are working on a rack-mounted model HMC, load the PC-Doctor from diskette using an external USB diskette drive, CD or selecting F12 during a system shut down and restart.

Note: If you are using a CD or diskette to load PC-Doctor, shut down and restart the HMC and wait until the PC-Doctor's main menu is displayed.

6. Click **Diagnostics** → **Other Devices** → **Modem** to perform the modem diagnostic test.
7. Did the diagnostic pass?
 - **No:** Go to step 8.
 - **Yes:** Go to 9 on page 241.
8. Is the modem connected correctly to a working telephone line (or equivalent)?

Note: This can be checked by connecting a known good telephone to the line in place of the modem and making a telephone call.

- **No:** Correctly connect the telephone line (or equivalent) to the modem. Go to step 1 on page 240. After completing the telephone line and modem verification test, continue with step 9.
- **Yes:** Go to step 9.

9. Verify the COM port by performing the following steps:

- a. Disconnect the modem cable from the COM port of the HMC.
- b. Select **Diagnostics** from the top menu.
- c. Select **System Ports** from the pull-down menu. The *SERIAL PORT TEST CATEGORY* screen displays.
- d. Ensure the following:
 - On desktop HMC models - IRQ numbers 4 and 3 are assigned to COM 1 and COM 2, and the planar to COM 2 connector cable is present and correctly installed.
 - On rack-mounted models - IRQ number 4 is assigned from COM 1.

Note: If the preceding information is not correct, the COM port might be disabled, or might be incorrectly configured. This can be resolved by accessing the setup utility (by pressing the F1 key) during power on.


- e. Ensure all diagnostics except "External Loopback" are selected
- f. Select **Run Screen** from the bottom menu.
- g. Ensure all selected diagnostics show Passed

Note: If any diagnostics fail, replace the planar.

10. Verify the external modem by performing the following steps:

- a. Reconnect the modem cable to the correct COM port.
- b. Ensure that the modem is powered on, connected to a working telephone line, and is securely cabled to the communications cable.
- c. Press Esc to return to the PC-Doctor main menu or shut down and restart the HMC.
- d. Select **Hardware Info** from the top menu
- e. Select **COM and LPT Ports** from the pull-down menu. The hardware query displays COM and LPT port information.
- f. Verify the following:
 - A modem was detected on the correct COM port
 - The modem test returned Passed
 - Dial tone: Detected
 - ATII: Displays the modem's model information

Note:

- a. If you were not able to get the desired results in step 10f, refer to the MultiTech MultiModem^{II} user's guide, installation guide, or reference guide for your modem. To access the MultiTech MultiModem^{II} documentation, go to the MultiTech  Web site at <http://www.multitech.com/documents/families/multimodemII/manuals.asp>.
- b. If necessary, after you have completed the MultiTech MultiModem^{II} documentation, come back here to complete the final step of this procedure.

11. Choose from the following options:

- If the modem was not detected, replace and verify the following customer replaceable parts in the order listed:
 - a. Communications cable
 - b. Modem

- If the modem test did not return with Passed, replace the modem.
- If the dial tone did not return with Detected, verify the telephone line operation then retest. If the failure reoccurs, replace the modem.

Testing the HMC's Ethernet adapter:

Use this procedure to test the Ethernet adapter in the HMC.

1. Is the Ethernet port currently functioning though normal operation of the HMC?
 - **No:** Go to step 2.
 - **Yes: This ends the procedure.**
2. Are the Ethernet configuration values set correctly? (IP address, subnet mask, and so on.)
 - **No:** Set the Ethernet configuration values to their correct settings. Then go back to step 1.
 - **Yes:** Go to step 3.
3. Can the IP address of the HMC be 'pinged' by another system that should be able to 'see' the HMC on the network?
 - **No:** Go to step 4.
 - **Yes:** Go to step 10.
4. Is the Ethernet cable attached correctly to the HMC and the network?
 - **No:** Attach the HMC to the network using an Ethernet cable with the correct pinout. Then go to step 1.
 - **Yes:** Go to step 5.
5. Is the Ethernet cable the correct pinout? (There are two types of Ethernet cables in use, which are distinguished by different pinouts. The network will determine which version of cable to use.)
 - **No:** Replace the Ethernet cable with the correct version. Then go to step 1.
 - **Yes:** Go to step 6.
6. Perform the following steps:
 - a. Install the PC-Doctor diskette into drive A of the HMC: (floppy drive).
 - b. Shut down and restart the HMC and wait until the PC-Doctor main menu is displayed.
 - c. To run the Ethernet diagnostics, select **Diagnostics** → **Other Devices** → **Intel Ethernet**.
Did the diagnostic pass?
 - **No:** Go to step 7.
 - **Yes:** Go to step 10.
7. Refer to the Ethernet hardware's hardware maintenance manual to determine if there are any internal settings or jumpers that might disable the Ethernet port.
Are there any internal settings or jumpers?
 - **No:** Go to step 8.
 - **Yes:** Go to step 9.
8. Replace the Ethernet hardware in the HMC. (This might be a PCI card or system board replacement, depending on the HMC hardware.) Go to step 1.
9. Set the internal settings/jumpers to enable the Ethernet port on the HMC. Go to step 1.
10. The failure does not seem to be in the HMC.

Testing the HMC's disk drive:

Use this procedure to test the disk drive in the HMC.

1. Did the disk drive test fail?
 - **No:** Go to step 5 on page 243.
 - **Yes:** Continue with the next step.

2. Perform the following steps:
 - a. Exchange the CRUs called by the diagnostics one at a time. For CRU removal and replacement instructions, refer to the PC hardware maintenance manual for the system on which you are working. See "Equivalent maintenance information for the HMC's personal computer hardware" on page 250 to access the hardware maintenance manual for your HMC personal computer model.
 - b. After each CRU is exchanged, test the repair using the information in "Performing system unit testing using PC-Doctor" on page 239. Select **Hard Disk Drive** problem area.
Did the disk drive test fail?
 - **No:** Continue with the next step.
 - **Yes:** Contact your next level of support.
3. Ensure the following and then continue with the next step:
 - If you exchanged the disk drive and there are jumpers or tab settings on the new disk drive, ensure that the settings are the same as the old drive.
 - If there is a SCSI cable-terminating resistor device, ensure it is secured to the cable and (if necessary) reattached to its original location on the PC.
Go to "Hard Disk Jumper Settings" in the PC hardware maintenance manual. See "Equivalent maintenance information for the HMC's personal computer hardware" on page 250 to access the hardware maintenance manual for your HMC personal computer model.
4. If you exchanged the disk drive, restore the HMC image to the new disk drive.
5. Use the information in "Performing system unit testing using PC-Doctor" on page 239 to test the PC. Select **Run All Selected** problem area.
 - If the tests fail, isolate the problem using the "Beginning HMC problem determination" on page 237 procedure.
 - If the tests run without errors, turn off the PC power and then turn on the power. Ensure that the system boots and the HMC screen displays. **This ends the procedure.**

Testing the HMC's DVD-RAM:

Use this procedure to test the DVD drive in the PC for the HMC.

1. Determine the media in the DVD-RAM drive:
 - Compact Disk Recordable (CD-R) similar to a CD
 - DVD-RAM media cartridgeIs the media a CD-R?
 - **No:** Go to step 4.
 - **Yes:** Continue with the next step.
2. Perform the following steps:
 - a. Clean the compact disk as follows:
 - Hold the disk by its edges. Do not touch the surface.
 - Remove dust and fingerprints from the surface by wiping from the center to the outside using a dry, soft cloth.
 - b. Reinstall the CD, with the label-side facing up.
 - c. Continue with the next step.
3. Retry the failing task using the original media.
Does the failure occur again?
 - **No:** Continue with the next step.
 - **Yes:** Go to step 4.**This ends the procedure.**
4. Ensure the write protect tab is in the "disabled" (down) position.

Was the write protect tab in the "disabled" (down) position?

- **No:** Go to step 3 on page 243.
- **Yes:** Continue with the next step.

5. Perform the following steps:

a. With the original media in the drive, note the following:

- If you are attempting a restore procedure, turn off the PC power.
- For any other operation, shut down the HMC, and then turn off the PC power.

Note: For shutdown procedures, see Powering on and off.

b. Turn on the PC power and test the DVD-RAM drive using the information in "Performing system unit testing using PC-Doctor" on page 239.

c. Select **DVD-RAM Drive** problem area.

d. When the test is complete, return here and continue with the next step.

6. Did the DVD-RAM test fail while testing with the original media?

- **No:** Go to step 1 on page 245.
- **Yes:** Continue with the next step.

7. Exchange the original media with a new one.

Note: If you are replacing DVD-RAM media, the new cartridge must be formatted. If possible, use another HMC to format the new cartridge.

8. Turn off the PC power.

9. Turn on the PC power, and test the DVD-RAM drive with the new media. Use the information in "Performing system unit testing using PC-Doctor" on page 239 to test the PC. Select **DVD-RAM Drive** problem area.

10. Did the DVD-RAM test fail while testing with the new media?

- **No:** The original media was defective. **This ends the procedure.**
- **Yes:** Continue with the next step.

11. Verify the following:

- All DVD-RAM drive data and power cables are secure.
- The DVD-RAM drive is jumpered as "master" and is cabled to the secondary IDE bus.

12. If the diagnostics continue to fail, exchange the DVD-RAM drive. When complete, run the DVD-RAM test again.

Note: If there are any jumpers or tab settings on the new drive, ensure that the settings match the old drive.

13. Did the DVD-RAM Drive test continue to fail?

- **No:** The original DVD-RAM drive was defective. **This ends the procedure.**
- **Yes:** Continue with the next step.

14. Continue exchanging CRU from the CRU list and running the DVD-RAM drive tests.

- If the CRUs fix the problem, this ends the procedure.
- If you cannot isolate the problem, call your next level of support for assistance.

15. The PC resources (for example: interrupt, I/O address) might be configured incorrectly. Verify the PC resources are correctly configured.

a. Select **System Unit** for the configuration area, and verify configuration for the system unit and all adapters.

b. When you complete the verification, retry the failing procedure and continue with the next step.

16. Does the failing procedure continue to fail?

- **No:** The resource settings were incorrect. **This ends the procedure.**

- **Yes:** If you cannot isolate the problem, contact your next level of support for assistance. **This ends the procedure.**


Testing the HMC's diskette drive:

Use this procedure to test the diskette drive in the PC for the HMC.

1. Perform the following steps:
 - a. Turn on the PC power and test the diskette drive using the information in "Performing system unit testing using PC-Doctor" on page 239.
 - b. Select **System Unit** problem area and the test of **Diskette Drive**.

Note: Do not test with the diskette on which the errors occurred. Use a new diskette.
 - c. When the test is complete, continue with the next step.
2. Did the diskette test fail while testing with a new diskette?
 - **No:** Go to step 7.
 - **Yes:** Continue with the next step.
3. Exchange the diskette drive and run the diskette test again.
4. Did the diskette test fail again?
 - **No:** The original diskette drive was failing. **This ends the procedure.**
 - **Yes:** Continue with the next step.
5. Continue exchanging CRUs from the CRU list and running tests. If the CRUs fix the problem, this ends the procedure.
6. Choose from the following options:
 - If the problem is resolved by replacing a CRU, this ends the procedure.
 - If you cannot resolve the problem, contact your next level of support for assistance. **This ends the procedure.**
7. Did the original failure occur while writing to a diskette?
 - **No:** Go to step 9.
 - **Yes:** Continue with the next step.
8. Retry the original task using a new diskette.
 - If the failure occurs again, go to step 11.
 - If no failures occur, the original diskette was failing. **This ends the procedure.**
9. Re-create the information on the diskette, or obtain a new diskette with the information.
10. Retry the original task.
 - If the failure occurs again, continue with the next step.
 - If no failures occur, the original diskette was failing. **This ends the procedure.**
11. Test the diskette drive, using the information in "Performing system unit testing using PC-Doctor" on page 239. Select **System Unit** problem area and the test of **Diskette Drive**.
 - If the tests fail, isolate the problem using the procedures found in the PC hardware maintenance manual. For additional PC maintenance information, see "Equivalent maintenance information for the HMC's personal computer hardware" on page 250 to access the hardware maintenance manual for your HMC personal computer model.

For the latest information regarding maintenance of your HMC PC, system board specifications, and parts, refer to the PC hardware maintenance manuals. The latest versions of these publications are available through the IBM Web site:

 - a. Go to the IBM  Web site at <http://www.ibm.com>.
 - b. Select **Support & downloads**.
 - c. In the Search Technical support field, type the order number of the manual you want to access.

- d. Click **Search**.
- e. In the search results, click the link for the document you want.
- If the tests do not isolate the problem, contact your next level of support for assistance.

Testing the HMC's display:

Use this procedure when you are having a display problem with the HMC.

1. Is the display type a 95xx (17P, 17X, 21P)?
 - **No:** Continue with the next step.
 - **Yes:** 95xx-xxx repairs might require replacing internal display CRUs. Repair and test the display using the procedures in *Monitor Hardware Maintenance Manual Vol 2, S41G-3317*.
2. Is the display type a 65xx (P70, P200)?
 - **No:** Continue with the next step.
 - **Yes:** 65xx-xxx repairs might require replacing the entire display. There are no internal display CRUs. Repair and test the display using the procedures in *Monitor Hardware Maintenance Manual Vol 3, P and G series, S52H-3679*.
When the test and repair are complete, continue with step 5.
3. Is the display type a 65xx (P72, P202)?
 - **No:** Continue with the next step.
 - **Yes:** 65xx-xxx repairs might require replacing the entire display. There are no internal display CRUs. Repair and test the display using the procedures in *Color Monitor Operating Instructions*.
When the test and repair are complete, continue with step 5.
4. Repair and test the display using the documentation included with the display. When the test and repair are complete, continue with step 6.
5. Verify the repair using the information in "Performing system unit testing using PC-Doctor" on page 239. Select **System Unit** for the problem area and the **Test for Display**.
When the test and repair are complete, continue to step 6.
6. Return the system to normal operations. **This ends the procedure.**

Maintaining the HMC

Learn about maintaining and servicing the HMC.

The HMC connects to one or more managed systems to perform various functions. The HMC's primary functions include the following:

- Providing a console for system administrators and service representatives to manage server hardware.
- Creating and maintaining a multiple partitioned environment on a managed system.
- Detecting, reporting, and storing changes in hardware conditions.
- Acting as a service focal point for service representatives to determine an appropriate service strategy.
- Displaying operating system session terminals for each partition.

The HMC system is delivered with its machine code preinstalled on the disk drive. After the system is installed and connected to a managed system, system management tasks can begin.

The HMC machine code does not have provisions for loading or running additional applications that are not related to hardware management or service. All the tasks you need to maintain the managed system, the underlying operating system, and the HMC's machine code are available by using the HMC's management interface.

Managed system operation:

The HMC's graphical user interface provides the functions needed to create and maintain a partitioned environment on a managed system. Using the interface allows for direct manipulation of HMC-defined objects and increased information regarding detected changes in hardware conditions.

The managed system can be run as a partitioned system, sometimes referred to as *logically partitioned*. This means that the managed system can run multiple operating systems simultaneously. The system can also run as a large single partition, which is known as the *manufacturing default configuration* when the system is delivered. If the system has been partitioned, then a the single partition that uses all the system resources is referred to as a *full system partition*.

Partitioning provides users with the ability to divide a single managed system into several systems. Each of these systems, running in a partition, is capable of running applications in multiple, independent environments simultaneously. Logical partitioning makes it possible for a user to run a single application using different sets of data on separate partitions, as if that application were running independently on separate physical systems. By creating partitions, for example, a company can test its programs in one partition while developing the same program in another, at the same time, all using the same system. This "same system" partitioning method is more cost-effective, potentially eliminating the need for a separate test system.

The full system partition is no different from the traditional way of using a system. The single server uses all of its resources as one system.

HMC system diagnostics:

Your HMC system also provides a set of diagnostic procedures that should be followed when troubleshooting HMC problems. For details on accessing the HMC diagnostics, see "HMC diagnostics overview" on page 248.

Powering on and off the HMC:

During the process of powering on, the HMC checks to see which managed systems are available and communicating with the console. To ensure that each managed system is available before you power on the HMC, managed systems must be in standby mode or actively operating. Standby mode is indicated by the OK shown in the operator panel after the managed system has the power connected and the initial tests are complete.

Note: If the managed system is in an emergency power off (EPOW) condition, the managed system must be brought to standby mode before the HMC can be used to power on the system.

To power on the HMC, do the following:

1. Press the Power button once to turn on the power.
2. When the system has finished the power-on self-test (POST), log in to the HMC.

Power off the HMC:

To power off the HMC, do the following:

1. Log in to the HMC and select **Power Off**.
2. The HMC shuts down any applications that are running, and then turns off the HMC.

Power-on self-test:

After power is turned on and before the operating system is loaded, the system does a power-on self-test (POST). This test performs checks to ensure that the hardware is functioning correctly before the

operating system is loaded. During the POST, codes indicating the progress of the POST might be displayed. After the POST is complete, the HMC operating machine code loads and a login prompt is displayed.

Specifications and system unit locations:

Your HMC system is based on a model of personal computer. For information about system specifications and system unit locations, use the appropriate personal computer hardware maintenance manuals, see “Equivalent maintenance information for the HMC’s personal computer hardware” on page 250.

HMC external AC power cable:

To avoid electrical shock, a power cable with a grounded attachment plug is provided. Use only properly grounded outlets.

Power cables used in the United States and Canada are listed by Underwriter’s Laboratories (UL) and certified by the Canadian Standards Association (CSA). These power cords consist of the following:

- Electrical cables, type ST
- Attachment plugs complying with National Electrical Manufacturers Association (NEMA) L6-30P
- Appliance couplers complying with International Electrotechnical Commission (IEC) Standard 320, Sheet C13 and C14

Power cables used in other countries consist of the following:

- Electrical cables, type HD21 or HD22
- Attachment plugs approved by the appropriate testing organization for the specific countries where they are used
- Appliance couplers complying with the International Electrotechnical Commission (IEC) Standard 320, Sheet C13 and C14

HMC diagnostics overview

Learn about the HMC diagnostic path and how to find additional information on the base hardware.

The first step to service a managed system or an attached HMC is to go to the “Beginning problem analysis” on page 219 procedure. You will then be directed to the appropriate documentation depending on the type of problem that is to be isolated and repaired.

If a problem is determined to be in your HMC system, you are directed to the “HMC problem analysis” on page 235 for diagnostic and repair information.

The HMC problem analysis procedure will guide you to the appropriate repair action. Occasionally, you will be directed to the maintenance documentation for the HMC’s base personal computer. When this occurs, the maintenance documentation for the personal computer is used to complete the repair action.

Connector and hard disk drive restrictions for the HMC

The following table contains connector and hard disk drive restrictions that you will need to know when cabling or adding hard disk drives to your HMC.

Table 5. Connector and hard disk drive restrictions for the HMC

HMC machine type, and model number	Connector restrictions for cabling an HMC
7310-CR2	<p>The following are not supported:</p> <ul style="list-style-type: none"> • Use of the parallel port Note: The HMC is a closed system and as such, the hardware is used in a limited manner. No device drivers or code support any peripheral devices that use a parallel port. • The C2T IN and ISM ports <p>The CR2 only supports a USB keyboard and mouse. When the keyboard and mouse are connected to any of the three USB connectors, the third unconnected USB connector is <i>not</i> supported.</p> <p>To view the location of each connector identified above, refer to Cabling the HMC, then scroll to the back view of the model you are cabling.</p>
7310-CR3	<p>The following are not supported:</p> <ul style="list-style-type: none"> • Use of the parallel port Note: The HMC is a closed system and as such, the hardware is used in a limited manner. No device drivers or code support any peripheral devices that use a parallel port. • Use of the HMC system management connector • Use of the serial port • Use of the DVD drive <p>The HMC supports only the USB keyboard and mouse that are shipped with the HMC. No other USB devices are supported when connecting to the third USB connector. There is no requirement that you must use a specific USB port for the keyboard and mouse. When a set of USB connectors is being used for a keyboard and mouse, all other USB and the PS/2 connectors are rendered inoperable. When the PS/2 connectors are being used for a keyboard and mouse, all USB connectors are rendered inoperable.</p> <p>To view the location of each connector identified above, refer to Cabling the HMC, then scroll to the back view of the model you are cabling.</p>
7310-C03	<p>The following are not supported:</p> <ul style="list-style-type: none"> • Use of the parallel port Note: The HMC is a closed system and as such, the hardware is used in a limited manner. No device drivers or code support any peripheral devices that use a parallel port. • Use of the audio connectors • Use of the diskette drive <p>The HMC supports only the USB keyboard and mouse that are shipped with the HMC. No other USB devices are supported when connecting to the third USB connector. There is no requirement that you must use a specific USB port for the keyboard and mouse. When a set of USB connectors is being used for a keyboard and mouse, all other USB and the PS/2 connectors are rendered inoperable. When the PS/2 connectors are being used for a keyboard and mouse, all USB connectors are rendered inoperable.</p> <p>To view the location of each connector identified above, refer to Cabling the HMC, then scroll to the back view of the model you are cabling.</p>

Table 5. Connector and hard disk drive restrictions for the HMC (continued)

HMC machine type, and model number	Connector restrictions for cabling an HMC
7310-C04	<p>The following are not supported:</p> <ul style="list-style-type: none"> • Use of the parallel port Note: The HMC is a closed system and as such, the hardware is used in a limited manner. No device drivers or code support any peripheral devices that use a parallel port. • Use of the serial connectors • Use of the audio connectors • Use of the diskette drive <p>The HMC supports only the USB keyboard and mouse that are shipped with the HMC. No other USB devices are supported when connecting to the third USB connector. There is no requirement that you must use a specific USB port for the keyboard and mouse. When a set of USB connectors is being used for a keyboard and mouse, all other USB and the PS/2 connectors are rendered inoperable. When the PS/2 connectors are being used for a keyboard and mouse, all USB connectors are rendered inoperable.</p> <p>To view the location of each connector identified above, refer to Cabling the HMC, then scroll to the back view of the model you are cabling.</p>
7310-C05	<p>The following are not supported:</p> <ul style="list-style-type: none"> • Use of the parallel port Note: The HMC is a closed system and as such, the hardware is used in a limited manner. No device drivers or code support any peripheral devices that use a parallel port. • Use of more than one hard disk drive <p>To view the location of each connector identified above, refer to Cabling the HMC, then scroll to the back view of the model you are cabling.</p>

Equivalent maintenance information for the HMC's personal computer hardware

The following table provides information to help cross-reference your HMC equivalent machine type and model number for the base personal computer. You can use the entries in this table to link directly to the base PC maintenance documentation.

Table 6. Equivalent maintenance information for the HMC's personal computer hardware






HMC machine type, and model number (available on the serial number plate of your HMC)	Equivalent base personal computer machine type and model number	Order numbers for supporting hardware maintenance information
7310-CR2 Note: For the latest HMC Parts information, go to Hardware management console (HMC) parts, then scroll to your HMC machine type and model.	Type 8676 Model 22X	To access the Type 8676 Hardware Maintenance Manual and Troubleshooting Guide, select 48p9908.pdf from the Support & downloads  Web site.
7310-CR3 Note: For the latest HMC Parts information, go to Hardware management console (HMC) parts, then scroll to your HMC machine type and model.	Type 8837 Model 22U	To access the Type 8837 Hardware Maintenance Manual and Troubleshooting Guide, select 25k8109.pdf from the Support & downloads  Web site.
7310-CR4	7978 Model 42U or 7978 Model PBT	31R1156

Table 6. Equivalent maintenance information for the HMC's personal computer hardware (continued)

HMC machine type, and model number (available on the serial number plate of your HMC)	Equivalent base personal computer machine type and model number	Order numbers for supporting hardware maintenance information
7310-C03 Note: For the latest HMC Parts information, go to Hardware management console (HMC) parts, then scroll to your HMC machine type and model.	Type 8187 Model F4U (without POV)	To access the Type 8187 Hardware Maintenance Manual, select 74p2661.pdf from the Support & downloads Web site.
7310-C04 Note: For the latest HMC Parts information, go to Hardware management console (HMC) parts, then scroll to your HMC machine type and model.	Type 8141 Model 31U	To access the Type 8141 Hardware Maintenance Manual, select 19r0486.pdf from the Support & downloads  Web site.
7310-C05 Note: For the latest HMC parts information, go to Hardware management console (HMC) parts, then scroll to your HMC machine type and model.	Type 8485 Model 3AU	To access the Type 8485 Problem Determination and Service Guide, select 31r205.pdf from the Support & downloads  Web site.
7310-C06	4362 Model 52U or 4362 Model PAT	nn1cqmst

For the latest information regarding the maintenance of your HMC personal computer, system board specifications, and parts, refer to the appropriate personal computer hardware maintenance manual. Use the links in the previous table to go to the personal computer hardware maintenance information on the World Wide Web. If you cannot link directly to these documents, you can access the documents by using the following procedure:

1. Go to the IBM  Web site at <http://www.ibm.com>.
2. Select **Support & downloads**.
3. In the Search Technical support field, type the *order number from the previous table* for the hardware maintenance information that you want to access.
4. Click **Search**.
5. In the search results, click the link for the appropriate document.

Diagnostics, test, and recovery

The following tools are available to help identify and resolve hardware-related problems:

- Power-on self-test (POST)
 - POST beep codes
 - Error code format
- 7310-CR4 sector disk drive scanning procedure

To do a sector by sector scan of your 7310-CR4 disk drive, do the following:

1. Power off then power on the HMC.
2. As the HMC is rebooting, watch the HMC display. After the second Broadcom Ethernet driver screen appears on your display, simultaneously press the "CTRL" key and the letter "A" key . An options menu appears on your display.
3. From the list of options select **Disk Utilities**.
4. Select **Disk Utilities**
5. Select **Verify Disk Media....**

Note: After selecting the Verify Disk Media.... the HMC will begin to do a sector by sector scan of you disk drive.

- PC-Doctor

Note: For additional information about items in the previous list, see the appropriate personal computer hardware maintenance manual. To access the personal computer hardware maintenance documentation, refer to the “Equivalent maintenance information for the HMC’s personal computer hardware” on page 250.

PC-Doctor

PC-Doctor is a set of diagnostic and system information tools included with the HMC. In rack-mounted HMC models, PC-Doctor is preinstalled on the system. PC-Doctor is included on the HMC Recovery CDs for Release 3 Version 3.0 (or later) for HMC models that are not rack-mounted.

Running PC-Doctor on an HMC that is not rack-mounted

Before accessing the PC-Doctor application on the HMC, you need to create a bootable diskette (referred to as the PC-Doctor diskette in the remainder of this section).

To create the diskette:

1. On a machine running Windows, insert a high-density floppy diskette in your diskette drive.
2. Insert volume 2 of HMC Recovery CD into the CD drive.
3. Select **Start > My Computer**.
4. Open the CD and go to the `pc_diag` directory.
5. Open the `readme` file and follow the instructions for creating the PC-Doctor diskette using the `pc_diag.exe` tool.

To run PC-Doctor:

1. Power off the HMC.
2. Insert the PC-Doctor diskette you created.
3. Power on the HMC.

If the HMC does not read the PC-Doctor diskette upon startup, it might be due to the startup sequence. To make the PC-Doctor diskette the primary startup media, do the following:

1. Power off the HMC.
2. Power on the HMC and press F1 when the Setup Utility prompts during startup.
3. Select the **Startup** tab.
4. Highlight **Startup Sequence** and press Enter.
5. Under **Primary Startup Sequence**, make sure the first startup device is set to **Removable**. Then follow the remainder of the instructions on the screen to complete the procedure.

Running PC-Doctor on a rack-mounted HMC

Note: A rack-mounted HMC has PC-Doctor preinstalled. You can upgrade your PC-Doctor using a bootable CD that has PC-Doctor installed. To use a bootable diskette copy of PC-Doctor on a rack-mounted HMC, you must use an external USB diskette drive.

To run PC-Doctor on a rack-mounted HMC:

1. Turn off the power to the HMC.
2. If you are using a bootable CD or diskette to run PC-Doctor, insert it into the appropriate drive.
3. Turn the power to the HMC back on and press F2 when the message F2 for Diagnostics is displayed.
4. If prompted, type the appropriate password, then press Enter.

5. Select either **Extended** or **Basic** from the top of the screen.
6. From the diagnostic screen, select the test you want to run from the list and then follow all instructions.

Note: For additional information about HMC diagnostics, go to the diagnostics section in the appropriate personal computer hardware maintenance manual. To access the personal computer hardware maintenance documentation, refer to “Equivalent maintenance information for the HMC’s personal computer hardware” on page 250.

Removing and replacing parts on the HMC

Learn how to remove and replace parts on the HMC.

You can do most of the procedures for the personal computer on which your HMC is based. This section contains instructions to help you access the procedures that are needed for removing and replacing parts on your HMC.

Note: Depending on the system configuration, when you are directed to exchange parts, run tests, or change configuration data, the interface to the managed systems will be unavailable. If possible, before starting any of these tasks, ensure that all system management tasks are completed and all critical data is backed up.

Attention: Removing power from an HMC might cause loss of data on the disk drives. If power must be removed, select **Power Off** from the HMC user interface. This action shuts down the operating system and turns off the power to the HMC. See “Power off the HMC” on page 247.

HMC maintenance procedures

The procedures in this section help you to perform maintenance tasks and to install updates to the HMC.

Attention: The system board, adapters, memory modules, and processor modules can be damaged by electrostatic discharge. If you are directed to exchange a part in an HMC, refer to the “Handling Electro-Static Discharge (ESD) Sensitive Devices” in the appropriate PC maintenance information manuals.

When you are referred to the hardware maintenance manual for the personal computer, use the hardware maintenance manual for the appropriate personal computer machine type. To access the personal computer hardware maintenance documentation, refer to the “Equivalent maintenance information for the HMC’s personal computer hardware” on page 250.

System board specifications

Your HMC system is based on one of the following personal computer machine types and models.

- 8676 Model 22X is used for the 7310-CR2
- 8837 Model 22U is used for the 7310-CR3
- 8187 Model F4U(without POV) is used for the 7310-C03
- 8141 Model 31U is used for the 7310-C04
- 8485 Model 3AU is used for the 7310-C05

To find documentation about the base HMC personal computer and its components, refer to “Equivalent maintenance information for the HMC’s personal computer hardware” on page 250.

Recovering the HMC

If the HMC has had a problem and you need to recover the HMC, the procedure can be found in Recovering the HMC.

Attention: This procedure will restore the HMC image onto the disk drive in the HMC personal computer. Before performing this procedure, contact HMC support and also ensure that there are backups for all critical console data.

Backup Profiles

Ensure that critical data which is stored on the HMC is also regularly maintained on backup media. The procedure can be found in Backing up critical HMC data.

HMC machine code updates

For information about updates or upgrades for the HMC machine code, refer to “Obtaining HMC machine code updates and upgrades” on page 121.

Recovering an HMC after replacing a disk drive

If you have to replace a disk drive, you will have to recover the HMC image and restore your stored profile data. Go to Recovering the HMC for more information.

Performing the firmware (BIOS/VPD) update procedure (after replacing the system board)

When you replace the system board, you should always perform the firmware update procedure for your HMC personal computer.

Attention: Refer to the information label located inside the system unit cover for any model-specific information.

To perform the firmware (BIOS/VPD) update procedure, perform the following steps:

1. To find documentation about the base HMC personal computer and its components, refer to “Equivalent maintenance information for the HMC’s personal computer hardware” on page 250.
2. Review the section in your HMC personal computer information for “Updating the firmware”.
3. Perform the procedures to update the new system board with the latest BIOS firmware.
4. Perform the procedures to update the Vital Product Data (VPD) information with the machine type, model, and serial number for the HMC.
5. Return the HMC to normal operations.

Related concepts

“Obtaining HMC machine code updates and upgrades” on page 121

Learn how to obtain HMC machine code updates and upgrades.

Analyzing HMC machine code problems

Learn about analyzing HMC machine code problems with the help of support personnel.

Only perform this procedure if your hardware service provider directs you to do so. The support organization uses the *pesh* command to look at the HMC’s internal machine code to determine how to fix a machine code problem. Only a service representative or service representative can access this feature.

Starting an xterm shell:

You might need to start an xterm shell to perform directed support from the support center. This might be required if the support center needs to analyze a system dump in order to better understand machine code operations at the time of a failure. To start an xterm shell, perform the following:

1. Open a terminal by right-clicking the background and selecting **Terminals** → **rshterm**.
2. Type the *pesh* command followed by the serial number of the HMC and press Enter.
3. You will be prompted for a password, which you must obtain from your next level of support.

Powering on managed systems after a power outage when your HMC is configured as a DHCP server

Learn how to correctly power on your managed systems after a power outage when your HMC is configured as a Dynamic Host Configuration Protocol (DHCP) server.

The following models require that your HMC be configured as a DHCP server:

- IBM System p5 575
- IBM eServer p5 590
- IBM eServer i5 and eServer p5 595

To power on your managed systems after a power outage, perform the following steps:

1. Choose from the following options:
 - If the location's main power *has not* been restored, go to step 2.
 - If the location's main power *has* been restored, perform the following steps:
 - a. Allow the servers and HMC to power on completely.
 - b. Log on to the HMC interface.
 - c. Continue with step 5.
2. Perform an Emergency Power Off (EPO) procedure on the servers. This can be completed in the following ways:
 - Using the ASMI. For details, see Performing an immediate power off .
 - Flipping the EPO switch on your managed system's Operator panel.
3. After the location's main power has been restored, power on the HMC.
4. After the HMC powers on and you have logged on to the HMC interface, restore base power to the managed systems by turning on the EPO switches on the managed systems.
5. Verify that the managed systems are powered on to the correct operating state.
 - a. In the Navigation area on the HMC interface, click **Server and Partition**.
 - b. In the Navigation area, select **Frame Management**.
 - c. In the Contents area, verify that the virtual operator panel displays Standby/Standby for each frame managed by your HMC.
 - d. In the Navigation area, select **Server Management**. The managed systems power on to the last state they were in when power was lost.
 - e. In the Contents area, verify that the virtual operator panel displays the correct operating state.

Note: For more information about other managed system operating states, see Managed system states.


6. Perform the following actions as necessary:
 - If your HMC is configured as a DHCP server, perform the actions listed in Verifying that your HMC DHCP private network is configured correctly.
 - If the virtual operator panel displays Version Mismatch in the Contents area, the HMC most likely has an IP connection identified as a one type of IP address, when in actuality the IP is communicating with another type of IP address. If Version Mismatch displays in the virtual operator panel, contact your next level of support for assistance.
 - If the system did not power on automatically, power on the managed system from the HMC. For more information, see Powering on a managed system.
7. Verify that I/O is assigned correctly.
 - a. In the Contents area, right-click the frame and select **Properties**.
 - b. In the Properties window, click the **I/O Units** tab.
 - c. Ensure that the I/O locations are correct by comparing the physical location code of the I/O unit on the left with the managed system serial number on the right.

8. Choose from the following options:

- If the I/O units are assigned correctly, your managed systems are powered on and ready for use.
- If the I/O units are assigned to an incorrect managed system, you have a network communication problem. Contact your next level of support for assistance.


Troubleshooting the keyboard, video, and mouse (KVM) switch for the 1x8 and 2x8 console manager

Learn about troubleshooting the KVM switch on a 1x8 and 2x8 Console Manager.

Use this procedure to isolate a problem on a 1x8 or 2x8 console manager. You will use this procedures in conjunction with the Console switch installation and user's guide  (680 KB) and the Local 2x8

Console manager user's guide  (6000 KB).

1. Choose from the following options:

- If you are troubleshooting a 1x8 console manager, continue with step 5.
- If you are troubleshooting a 2x8 console manager, refer to the Local 2x8 Console manager user's guide  (6000 KB) and run the onboard diagnostics. When finished, return here and continue with step 2.

2. Do the onboard diagnostics for the 2x8 Console Manager report any problems, or were you unable to run the diagnostics?

- **No:** Continue with step 3.
- **Yes:** Continue with step 5.

3. Do the onboard diagnostics of the 2x8 console manager indicate a no firmware cyclical redundancy check (CRC) error?

- **No:** To download the latest firmware updates onto your KVM switch, go to Local 2x8 Console manager User's Guide. Then return here and continue with step 5.
- **Yes:** Continue with step 4.

4. Do the onboard diagnostics indicate that there are no conversion option (CO) cables that are suspect?

- **No:** Replace the CO cable that caused a problem, then go to 5.
- **Yes:** Continue with step 5.

5. Is the monitor blank?



- **No:** Continue with the next step.
- **Yes:** Refer to "Troubleshooting monitor problems when connected to a KVM switch for the 1x8 and 2x8 console manager" on page 257.

6. Is your keyboard input recognized?

- **No:** Refer to "Troubleshooting keyboard problems when connected to a KVM switch for the 1x8 or 2x8 console manager" on page 258.
- **Yes:** Continue with the next step.

7. Can the OSCAR menu be displayed?

Note: For more information on using the OSCAR interface, which uses step by step menus that allow you to view, configure and select target devices connected to the KVM switch, refer to the following user guides:

- Console switch installation and user's guide  (680 KB)
- Local 2x8 Console manager user's guide  (6000 KB)

- **No:** Refer to “Troubleshooting user port problems for the (KVM) switch on a 1x8 or 2x8 console manager” on page 259.
 - **Yes:** Continue with the next step.
8. Is the KVM switch powering on?



Note: Check the green power LED that is located on the front of the KVM switch, approximately 2 in. to the right of the power on/off switch.

- **No:** Refer to “Troubleshooting a power problem for the KVM switch on the 1x8 or 2x8 console manager” on page 259
- **Yes: This ends the procedure.**

Troubleshooting monitor problems when connected to a KVM switch for the 1x8 and 2x8 console manager

Use this procedure to diagnose monitor problems when the monitor is connected to a KVM switch on a 1x8 or 2x8 Console Manager.

Before beginning this isolation procedure, invoke the OSCAR interface on your monitor, as described in “Starting the OSCAR interface”. Information on using OSCAR can be found in your Console switch

installation and user’s guide  (680 KB) or Local 2x8 Console manager user’s guide  (6000 KB). The OSCAR interface uses step by step menus that appear on your monitor allowing you to view, configure and select target devices connected to the KVM switch.

1. Can you start OSCAR?
 - **No:** Go to “Troubleshooting user port problems for the (KVM) switch on a 1x8 or 2x8 console manager” on page 259.
 - **Yes:** Go to step 2.
2. Are there any servers that, when selected from OSCAR, display on the monitor?
 - **No:** Go to step 4.
 - **Yes:** Go to step 3.
3. On servers that do not display, is the conversion option (CO) cable connected correctly to the graphics adapter?
 - **No:** Reseat the cable and check the monitor.
 - **Yes:** Go to step 5.
4. Is your monitor cable seated correctly at the KVM switch?
 - **No:** Reseat the cable and check the monitor.
 - **Yes:** Go to step 6.
5. Is your monitor refresh rate set at or below 1280 x 1024 resolution?
 - **No:** Set the refresh rate at or below 1280 x 1024.
 - **Yes:** Go to step 8 on page 258.
6. Perform the following steps:
 - a. Connect a different monitor to the same user port on the KVM switch.
 - b. Ensure both switch and monitor are plugged in and powered on (green LED indicates power on) and that the correct monitor input is selected.

Is the monitor still blank?

 - **No:** Follow the problem determination guide for the monitor you replaced.
 - **Yes:** Go to step 7.
7. Power cycle your KVM switch by toggling the On/Off switch back and forth, ending with the On/Off switch in the “On” position.

Is your monitor still blank?

- **No: This ends the procedure.**
 - **Yes:** Replace the KVM switch.
8. Is your server powered on?
- **No:** Power on the server.
 - **Yes:** Go to step 9.
9. Replace the KVM conversion option (KCO) or the USB conversion option (UCO). This will be dependent on the option that is in use and connects to your server.
- Is the monitor still blank?
- **No: This ends the procedure.**
 - **Yes:** Go to step 10.
10. Change the port on your KVM switch to which the CAT5 cable going to the KCO or to the UCO is attached.
- Is the monitor still blank?
- **No: This ends the procedure.**
 - **Yes:** Replace the KVM switch.

Troubleshooting keyboard problems when connected to a KVM switch for the 1x8 or 2x8 console manager

Learn about troubleshooting the KVM switch on a 1x8 and 2x8 Console Manager.

Before beginning this isolation procedure, invoke the OSCAR interface on your monitor. The OSCAR interface uses step-by-step menus allowing you to view, configure and select target devices connected to your KVM switch. Information on using OSCAR can be found in your Console switch installation and



user's guide  (680 KB) or Local 2x8 Console manager user's guide  (6000 KB).

1. Does your keyboard invoke OSCAR?
 - **No:** Go to step 4.
 - **Yes:** Go to step 2.
 2. When selected, do any of your powered on servers accept input from the keyboard?
 - **No:** Go to step 4.
 - **Yes:** Go to step 3.
 3. Is the cable connected properly to the PS/2 or USB port on the server that does accept keyboard input?
 - **No:** Reseat the cable and check the keyboard.
 - **Yes:** Go to step 7 on page 259.
 4. Is the keyboard seated correctly at the KVM switch?
 - **No:** Reseat the cable and check the keyboard.
 - **Yes:** Go to step 5.
 5. Connect a different keyboard to the same user port on the KVM switch. Ensure the keyboard cable is correctly seated.
- Is your keyboard now functioning?
- **No:** Follow the problem determination guide for the keyboard you replaced.
 - **Yes:** Go to step 6.
6. Power cycle your KVM switch by toggling the On/Off switch back and forth, ending with the On/Off switch in the "On" position.
- Is the keyboard working?
- **No:** Replace the KVM switch.
 - **Yes: This ends the procedure.**

7. Replace the KVM conversion option (KCO) or the USB conversion option (UCO). This will be dependent on the option that is in use and connects to your server.
Is your keyboard working?
 - **No:** Go to step 8.
 - **Yes: This ends the procedure.**
8. Change the port on your KVM switch to which the CAT5 cable going to the KCO or to the UCO is attached.
Is your keyboard working?
 - **No:** Replace the KVM switch.
 - **Yes: This ends the procedure.**

Troubleshooting user port problems for the (KVM) switch on a 1x8 or 2x8 console manager

Learn about troubleshooting the user port for the KVM switch on a 1x8 and 2x8 Console Manager.

1. Is your keyboard properly connected to your KVM switch?
 - **No:** Properly connect the keyboard to your KVM switch and invoke the OSCAR interface.
 - **Yes:** Go to step 2.
2. Connect a different keyboard to the switch.
Was the OSCAR interface successfully invoked?
 - **No:** Go to step 3.
 - **Yes: This ends the procedure.**
3. Connect the keyboard and the monitor to different user ports on the KVM switch.
Was the OSCAR interface successfully invoked?
 - **No:** Go to step 4.
 - **Yes:** The KVM Switch has bad user ports. Replace the KVM switch.
4. Power cycle your KVM switch by toggling the On/Off switch back and forth, ending with the On/Off switch in the "On" position.
Was the OSCAR interface successfully invoked?
 - **No:** Go to step 5.
 - **Yes: This ends the procedure.**
5. Download the latest firmware to the KVM switch via a serial connection. Depending on the KVM switch model you are servicing refer to either the Console switch installation and user's guide  (680 KB) or the Local 2x8 Console manager user's guide  (6000 KB) for information on downloading firmware updates.
Was the OSCAR interface successfully invoked?
 - **No:** Replace the KVM switch.
 - **Yes: This ends the procedure.**

Troubleshooting a power problem for the KVM switch on the 1x8 or 2x8 console manager

Learn about troubleshooting a power problem for the KVM switch on a 1x8 or 2x8 Console Manager.

1. When you power on your KVM switch does the green power LED light up?
 - **No:** Check that the power cable is properly connected to the power source and the KVM switch. Then go to step 2.
 - **Yes: This ends the procedure.**
2. Was the power cable seated correctly to the power source and the KVM switch?

- **No:** Reseat the power cable connection to the power source and the KVM switch. Then go to step 3.
 - **Yes:** Continue with step 3.
3. Power on your KVM switch.
Does the green power LED light up?
- **No:** Power down the KVM switch and replace the power cable to the KVM switch. Then go to step 4.
 - **Yes: This ends the procedure.**
4. Power on your KVM switch.
Does the green power LED light up?
- **No:** Power down the KVM switch and connect the KVM switch to a different power source. Then go to step 5.
 - **Yes: This ends the procedure.**
5. Power on your KVM switch.
Does the KVM switch power on?
- **No:** Replace the KVM switch.
 - **Yes: This ends the procedure.**

Collecting reference codes and system information

Learn how to collect reference codes and other system information.

The reference codes and system information can help determine the correct solution to fix a problem. The reference codes and system information can appear on the HMC or on the server's control panel. If you have logical partitions, you will need to use the HMC.

Note: Ensure you have a printed copy of the appropriate problem reporting form to document the information you collect here. For details, see "Using the problem reporting forms" on page 443.

Using the HMC to collect reference codes and system information

Learn how to collect reference codes and other system information with an HMC.

Perform these steps to collect reference codes (functions 11-19) and system information (function 20) on an HMC.

Note: Ensure you have a printed copy of the appropriate problem reporting form to document the information you collect here. For details, see "Using the problem reporting forms" on page 443.

1. In the navigation area, expand **Server and partition** → **Server Management**.
2. To view the reference code that corresponds to function 11 on the control panel: In the contents area, select the system or logical partition and view the associated value in the Operator panel value column.
3. To view reference codes that correspond to function 12-19 on the control panel: In the contents area, expand the system.
4. Select the system or logical partition.
5. Right-click the system or logical partition and select **Properties**.
6. Select the **Reference Code** tab.
7. Select the entry that corresponds to the time stamp you want to view.
8. Click the **Details** button.
9. Record the values that correspond to functions 12 through 19 on the control panel.
10. When finished, click **OK** twice.

11. To collect system information that corresponds to function 20 on the control panel: In the navigation area, open the **Service Applications** folder.
12. Select **Service Focal Point**.
13. In the contents area, select **Service Utilities**.
14. In the Service Utilities window, select the system and select **Selected** → **Operator Panel Service Functions**.
15. Choose from the following options:
 - To view function 20 for the selected system, select **System Function** → **System Type, Model, and Feature Code (20)**.
 - To view function 20 for a logical partition, select the logical partition from the list and select **System Function** → **System Type, Model, and Feature Code (20)**.
16. Record the machine type, model, processor feature code, and IPL type information.

For additional details on how to perform control panel functions on the HMC, see Accessing the control panel functions using the HMC.

Using the Integrated Virtualization Manager to collect reference codes and system information

Learn how to use the Integrated Virtualization Manager to collect reference codes and other system information.

Note: Ensure you have a printed copy of the appropriate problem reporting form to document the information you collect here. For details, see “Using the problem reporting forms” on page 443.

Choose the method you plan to use:

For details on collecting reference codes using the Integrated Virtualization Manager, see Viewing partition reference codes.

Using the control panel to collect reference codes and system information

Learn how to use the control panel to collect reference codes and other system information.

Follow these steps to collect reference codes and system information (functions 11 through 20) using the control panel:

Note: Ensure you have a printed copy of the appropriate problem reporting form to document the information you collect here. For details, see “Using the problem reporting forms” on page 443.

1. On the control panel, press the increment button until 11 is shown on the Function/Data display.
 - a. Press Enter.
 - b. Record the 32-character code: 16 characters from the first line, and 16 characters from the second line of the Function/Data display.
2. Press the increment button until 12 is shown on the Function/Data display.
 - a. Press Enter.
 - b. Record the 32-character code.
3. Press the increment button until 13 is shown on the Function/Data display.
 - a. Press Enter.
 - b. Record the 32-character code.
4. Press the increment button until 14 is shown on the Function/Data display.
 - a. Press Enter.

- b. Record the 32-character code.
5. Press the increment button until 15 is shown on the Function/Data display.
 - a. Press Enter.
 - b. Record the 32-character code.
6. Press the increment button until 16 is shown on the Function/Data display.
 - a. Press Enter.
 - b. Record the 32-character code.
7. Press the increment button until 17 is shown on the Function/Data display.
 - a. Press Enter.
 - b. Record the 32-character code.
8. Press the increment button until 18 is shown on the Function/Data display.
 - a. Press Enter.
 - b. Record the 32-character code.
9. Press the increment button until 19 is shown on the Function/Data display.
 - a. Press Enter.
 - b. Record the 32-character code.
10. Press the increment button again until 20 is shown on the first line of the Function/Data display.
 - a. Press Enter.
 - b. Record the machine type, model, and serial number that is shown.

Note:

1. If 11 is shown in the Function/Data display on the control panel display, the numbers that follow are the reference codes.
2. If a number other than 11 is shown in the Function/Data display, the number might not indicate a problem with the system. These reference codes might indicate functions you select from the control panel display.
3. If you have a console with Type and Reference Code columns on it, record the data under the Type column as the first 4 characters of function 11 on the problem reporting form. For details, see “Using the problem reporting forms” on page 443. If an A, B, C, or D is displayed as the first character in the Type column, use the data in the Reference Code column as the last 4 characters of function 11. For information about who to contact if you need more help, refer to “Contacting IBM service and support” on page 447.

Using AIX tools to collect reference codes and system information

Learn how to use AIX tools to collect reference codes and other system information.

Note: Ensure you have a printed copy of the appropriate problem reporting form to document the information you collect here. For details, see “Using the problem reporting forms” on page 443.

1. Log in as root user, or use CE login.
2. At the command line, type `diag` and press Enter.
3. From the Function Selection menu, select **Task Selection** and press Enter.
4. Select **Display Previous Diagnostic Results** and press Enter.
5. From the Display Previous Diagnostic Results display, select **Display Diagnostic Log Summary**. The Display Diagnostic Log is displayed showing a chronological list of events.
6. Look in the **T** column for the most recent **S** entry.
7. Select this row in the table and press Enter.
8. Choose **Commit**. The details of this log entry are shown.
9. Record the SRN value shown near the end of the entry.

10. Exit to the command line.

Using i5/OS tools to collect reference codes and system information

Learn how to use i5/OS tools to collect reference codes and other system information.

Use this procedure to learn how to search the service action log for an entry that matches the time, reference code, or resource of the reported problem and then activate the indicator light for the failing part.

Note: Ensure you have a printed copy of the appropriate problem reporting form to document the information you collect here. For details, see “Using the problem reporting forms” on page 443.

1. Be sure that you log in with service level authority.
2. On the command line of the i5/OS session, type `strsst` and press Enter.
3. Type your service tools user ID and service tools password on the System Service Tools (SST) Sign On display and press Enter.

Note: The service tools password is case-sensitive.

4. Select **Start a service tool** from the System Service Tools (SST) display. Press Enter.
5. Select **Hardware service manager** from the Start a Service Tool display and press Enter.
6. Select **Work with service action log** from the Hardware Service Manager display and press Enter.
7. On the Select Timeframe display, change the **From: Date and Time** to a date and time prior to when you began having the problem.
8. Search for an entry that matches one or more conditions of the problem:
 - Reference code
 - Resource
 - Date/Time
 - Failing item list
9. Select option 2 (Display failing item information) to display the service action log entry.
10. Select option 2 (Display details) to display location information. The information displayed in the date and time fields is the date and time for the first occurrence of the specific reference code for the resource displayed during the time range selected.
11. Record the information.

Using Linux tools to collect reference codes and system information

Learn how to use Linux tools to collect reference codes and other system information.

Note: Ensure you have a printed copy of the appropriate problem reporting form to document the information you collect here. For details, see “Using the problem reporting forms” on page 443.

For details, see Identify a failing part on a Linux system or logical partition.

Reference codes list for customers

Learn more about the various types of reference codes and how they can help with problem analysis.

To use reference codes effectively, you must use them in conjunction with other service and support procedures. If you were not directed here by another procedure, see “Beginning problem analysis” on page 219.

Use these codes to locate the reference code you are receiving. The xxxx can be any number 0 through 9 or letter A through F. The codes are grouped in ranges, although the recovery for each range might not

apply to every reference code within the range. If you cannot find your code range, contact your next level of support or your hardware service provider for help interpreting what it means.

If your code is 5 characters in length, or contains a hyphen (-), then it is a service request number (SRN). For details, refer to “Service request numbers (SRNs)” on page 405.

The reference codes are organized by their first character, with numbers preceding letters. To navigate this listing, click the number or letter that matches the first character of your code. Then select your code, if available, from the list provided.

Note: The 8-digit references codes will be displayed as xxxxxxxx on your control panel or interface. For ease of reading, there is a space between the first 4 and last 4 digits in this documentation.

0 2 3 4 6 7 9 A B C D E H V #

0

Table 7. Reference codes that start with 0.

Reference code	Description/Action
0xxxxx	A <i>No Connection</i> state occurred on a system managed by an HMC. Refer to “0xxxxx connection error codes” on page 271.

2

Table 8. Reference codes that start with 2.









Reference code	Description/Action
20A8xxxx	See (20A8, 20Dx, 20EE, 20FF, 2102, 220x, 25Ax, 25Cx, 2602, 2803, 2B2x) Model 185 and A50 reference (error) codes  .
20Dxxxxx	See (20A8, 20Dx, 20EE, 20FF, 2102, 220x, 25Ax, 25Cx, 2602, 2803, 2B2x) Model 185 and A50 reference (error) codes  .
20EExxxx	See (20A8, 20Dx, 20EE, 20FF, 2102, 220x, 25Ax, 25Cx, 2602, 2803, 2B2x) Model 185 and A50 reference (error) codes  .
20FFxxxx	See (20A8, 20Dx, 20EE, 20FF, 2102, 220x, 25Ax, 25Cx, 2602, 2803, 2B2x) Model 185 and A50 reference (error) codes  .
2102xxxx	See (20A8, 20Dx, 20EE, 20FF, 2102, 220x, 25Ax, 25Cx, 2602, 2803, 2B2x) Model 185 and A50 reference (error) codes  .
220xxxxx	See (20A8, 20Dx, 20EE, 20FF, 2102, 220x, 25Ax, 25Cx, 2602, 2803, 2B2x) Model 185 and A50 reference (error) codes  .
25Axxxxx	See (20A8, 20Dx, 20EE, 20FF, 2102, 220x, 25Ax, 25Cx, 2602, 2803, 2B2x) Model 185 and A50 reference (error) codes  .
25Cxxxxx	See (20A8, 20Dx, 20EE, 20FF, 2102, 220x, 25Ax, 25Cx, 2602, 2803, 2B2x) Model 185 and A50 reference (error) codes  .

Table 8. Reference codes that start with 2. (continued)

Reference code	Description/Action
2602xxxx	See (20A8, 20Dx, 20EE, 20FF, 2102, 220x, 25Ax, 25Cx, 2602, 2803, 2B2x) Model 185 and A50 reference (error) codes  .
2803xxxx	See (20A8, 20Dx, 20EE, 20FF, 2102, 220x, 25Ax, 25Cx, 2602, 2803, 2B2x) Model 185 and A50 reference (error) codes  .
2B2xxxxx	See (20A8, 20Dx, 20EE, 20FF, 2102, 220x, 25Ax, 25Cx, 2602, 2803, 2B2x) Model 185 and A50 reference (error) codes  .
26443136	It might indicate a software installation error. For more information, see Common SRCs for software installation.



3

Table 9. Reference codes that start with 3.

Reference code	Description/Action
3490xxxx	It might indicate a tape unit problem. See “Recovering from a tape or CD drive problem” on page 230.
3494xxxx	It might indicate a tape library problem. See “Recovering from a tape or CD drive problem” on page 230.
3570xxxx	It might indicate a tape unit problem. See “Recovering from a tape or CD drive problem” on page 230.
358xxxxx	It might indicate a tape unit problem. See “Recovering from a tape or CD drive problem” on page 230.
359xxxxx	It might indicate a tape unit problem. See “Recovering from a tape or CD drive problem” on page 230.

4

Table 10. Reference codes that start with 4.

Reference code	Description/Action
40xxxxxxx	See (40xx) Model 185 and A50 reference (error) codes  .
4685xxxx	It might indicate a tape or tape library problem. See “Recovering from a tape or CD drive problem” on page 230.
4B20xxxx	See (4B20) Model 185 and A50 reference (error) codes  .


6

Table 11. Reference codes that start with 6.

Reference code	Description/Action
63xxxxxx	It might indicate an CD drive error. See “Recovering from a tape or CD drive problem” on page 230.



7

Table 12. Reference codes that start with 7.

Reference code	Description/Action
7207xxxx	It might indicate a CD drive error. See "Recovering from a tape or CD drive problem" on page 230.
7208xxxx	See (7208) Tape drive reference codes  . The information in this topic is intended for service providers.

9

Table 13. Reference codes that start with 9.

Reference code	Description/Action
9348xxxx	See (9348) Tape unit reference codes  . The information in this topic is intended for service providers.
9427xxxx	See (9427) Tape unit reference codes  . The information in this topic is intended for service providers.

A

Table 14. Reference codes that start with A.





Reference code	Description/Action
A1xxxxxx	See (A1xx) Service processor reference (attention) codes  . Most of the information in this topic is intended for service providers.
A2xxxxxx	It might indicate a logical partition error. See (A2xx, B2xx) Logical partition reference codes  . The information in this topic is intended for service providers.
A6xxxxxx	Check the following for a specific A6xx reference code. If you do not see your reference code, it might indicate a Licensed Internal Code error was detected. See Common SRCs for software installation for more information.
A6xx0277	A compression disk unit cannot complete an operation. <ol style="list-style-type: none"> Do not turn off the system. Look at the 4 characters that are to the left of the Data display of function 17. These 4 characters indicate the type of problem that exists and the recovery action to perform. Is this numeral 8402 or 2002? <ul style="list-style-type: none"> No: Continue with the next step. Yes: The compression disk unit is temporarily full of data. The command to the compression disk is being held. When the subsystem controller has created sufficient space on the compression disk unit to contain the data, the command that is being held is released and the system resumes normal processing. If the system does not resume normal processing within 20 minutes, contact your next level of support or your hardware service provider. If this numeral is 8400 or 2000, the compression disk unit is full of data. The command to the compression disk is being held. <p>Go to "Disk unit full considerations" in the Backup and Recovery  book.</p>
A60011xx	It might indicate a software installation error. See Common SRCs for software installation for more information.

Table 14. Reference codes that start with A. (continued)





Reference code	Description/Action
A6xx500x	It might indicate a workstation controller error. See “Recovering from a workstation failure” on page 229.
A60050xx	It might indicate an Operations Console error. See Troubleshoot system reference code (SRC) data for Operations Console.
A900xxxx	It might indicate an Operations Console error. See Troubleshoot system reference code (SRC) data for Operations Console.
A9002000	<p>If the IPL completed normally, does the console have a signon? Note: If the console did not vary on, see “Recovering when the console does not show a sign-on display or a menu with a command line” on page 231.</p> <ol style="list-style-type: none"> If the system completed the IPL, check the QSYSARB job log for a message, and follow the corrective actions indicated. To view the QSYSARB job log: <ol style="list-style-type: none"> Use the Work with Active Jobs (WRKACTJOB) command, and then type 5 (Work with) next to the QSYSARB job. Select Option 10 (Display jobs) to view the job log. You need *QSECOFR user class, or *ALLOBJ and *JOBCTL special authority to view the job log. If the problem persists, contact your next level of support or your hardware service provider.
A9003610	<p>The system job tables are full for i5/OS.</p> <p>Use the following actions to make more job table entries available:</p> <ul style="list-style-type: none"> Delete unneeded spooled files. End unneeded jobs on job queues. Change the QMAXJOB system value to increase the maximum number of jobs allowed. Remove pending job logs with the Work with Job Logs (WRKJOBLOG) command or with the Remove Pending Job Log (QWTRMVJL) API. <p>Perform the following actions if you are not already signed on or are unable to sign on:</p> <ul style="list-style-type: none"> Power the system off and perform a manual IPL. Use the “Define or Change the System at IPL” menu to change the QMAXJOB system value to increase the maximum number of jobs allowed.
A90036A0	<p>A system job failed.</p> <p>Certain system functions might not be available. Perform the following actions to recover:</p> <ul style="list-style-type: none"> Shut down the system and perform an IPL. If the problem persists, contact your next level of support.
AAxxxxxx	<p>See the (AAxx) Partition firmware reference (attention) codes . The information in this topic is intended for service providers.</p>
ACT01503	An internal error has occurred. If possible an error log has been taken and if configured, the problem has been automatically reported. If the problem continues, contact your service representative.

B

Table 15. Reference codes that start with B.

Reference code	Description/Action
B0xxxxxx	Check the following for a specific B0xx reference code. If you do not see your reference code, it might indicate a communications error.

Table 15. Reference codes that start with B. (continued)

Reference code	Description/Action
B1xxxxxx	Check the following for a specific B1xx reference code. If you do not see your reference code, it might indicate one of the following: <ul style="list-style-type: none"> A service processor firmware error. For details, see (B1xx) Service processor firmware reference codes . The information in this topic is intended for service providers. An IPL load device error. For possible IPL load device errors, see “Recovering from IPL or system failures” on page 229.
B1xx45xx	It might indicate a software installation error. For details, see Common SRCs for software installation.
B2xxxxxx	See (A2xx, B2xx) Logical partition reference codes  . The information in this topic is intended for service providers.
B3xxxxxx	See (B3xx) Connection monitoring reference codes  . The information in this topic is intended for service providers.
B6xxxxxx	Check the following for a specific B6xx reference code. If you do not see your reference code, it might indicate a Licensed Internal Code or hardware event was detected. If the reference code is in the Problem Log or the Service Action Log, then it requires service and you should contact your next level of support or your hardware service provider.
B600500x	It might indicate an Operations Console error. See Troubleshoot system reference code (SRC) data for Operations Console.
B6081105	It might indicate a software installation error. See Common SRCs for software installation for more information.
B9xxxxxx	Check the following for a specific B9xx reference code. If you do not see your reference code, it might indicate an i5/OS IPL error. See “Recovering from IPL or system failures” on page 229.
B9003121	It might indicate a software installation error. See Common SRCs for software installation for more information.
BAxxxxxx	See the (BAxx) Partition firmware reference (error) codes  . The information in this topic is intended for service providers.

C

Table 16. Reference codes that start with C.













Reference code	Description/Action
C1xxxxxx	See (C1xx) Service processor progress codes (checkpoints)  . The information in this topic is intended for service providers.
C2xxxxxx	See (C2xx) Virtual service processor progress codes  . The information in this topic is intended for service providers.
C3xxxxxx	See i5/OS IPL status codes  . The information in this topic is intended for service providers.
C5xxxxxx	See i5/OS IPL status codes  . The information in this topic is intended for service providers.

Table 16. Reference codes that start with C. (continued)

Reference code	Description/Action
C6xxxxxx	See i5/OS IPL status codes  . The information in this topic is intended for service providers.
C7xxxxxx	These reference codes show the status of the server firmware IPL. For details, see Server firmware IPL status progress codes  . The information in this topic is intended for service providers.
C9xxxxxx	See (C900) i5/OS IPL status progress codes  . The information in this topic is intended for service providers.
CAxxxxxx	See the (CAxx) Partition firmware progress codes  . The information in this topic is intended for service providers.
Comm 65x	When using a virtual terminal (VTERM), you might see an error code displayed in the bottom-left corner of the VTERM window. For a list of the error codes and recovery actions, see the “Virtual terminal errors (Comm) error codes” on page 404.



D

Table 17. Reference codes that start with D.

Reference code	Description/Action
D1xxxxxx	<p>These codes can show progress or dump status. See either:</p> <ul style="list-style-type: none"> • (D1xx) Service processor progress codes (service processor dump and platform dump) . • (D1xx) Service processor status progress codes . <p>The information in these topics is intended for service providers.</p>
D2xxxxxx	<p>Show the status of an IPL or a system shutdown process. This is a normal indication while the panel functions and system code are shutting down the system.</p> <p>See the IPL SRC finder. Then perform the procedure in “Recovering from IPL or system failures” on page 229.</p>
D6xxxxxx	See (D6xx) General status progress codes  . The information in this topic is intended for service providers.
D9xxxxxx	See (D9xx) General status progress codes  . The information in this topic is intended for service providers.
DAxxxxxx	<p>These reference codes show the status of an IPL.</p> <p>For details, see the IPL SRC finder. Then perform “Recovering from IPL or system failures” on page 229.</p>
DLPAR_REM_FAIL_REASON	A trunk priority value that was not valid was specified.

E

Table 18. Reference codes that start with E.

Reference code	Description/Action
E2xxxxxx	Refer to (E2xx) Licensed Internal Code reference codes  .
E3xxxxxx	Refer to (E3xx) Licensed Internal Code reference codes  .
ERR_CONC_MINT_RMC_CMD_EXCEPTION	{0} operation for {1} resource has failed on partition {2}.
ERR_CONC_MAINT_RMC_CMD_ERROR_NO_OUT	{0} operation for {1} resource has failed on partition {2}. The partition standard output/error is not available.
ERR_CONC_MAINT_RMC_CMD_ERROR	{0} operation for {1} resource has failed on partition {2}. The partition standard output is: {2} The partition standard output is: {3} The partition standard error is: {4}
ERR_CONC_MAINT_RMC_AIX_CMD_ERROR	{0} operation for {1} resource has failed on partition {2}. The partition command is: {3} The partition standard output is: {4} The partition standard error is: {5}

H

Table 19. Reference codes that start with H.

Reference code	Description/Action
HCA_RELATED_FAILURE	The command failed during an HCA related operation.
HCA_DUPLICATE	The specified HCA data {0} is not valid because it has been assigned to the profile already. Select another adapter or remove the current assignment of the adapter and retry the operation.
HCA_INVALID_INPUT	The specified HCA data {0} is not valid for the operation. Either the adapter ID or GUID does not exist, the resource capability is not valid, or the data is not in the format 'Adapter ID/GID/Capabilities'. Correct and retry the operation.
HCA_UNSUPPORTED	i5/OS partitions do not support HCA adapter in this release. Remove the HCA adapter and retry the operation.
HSCxxxxx	Indicates an HMC message. For details, see "HMC error codes" on page 271.


V

Table 20. Reference codes that start with a V.

Reference code	Description/Action
VALIDATE_SYS_PROF_*	Follow the actions that are displayed with the reference code.

#

Table 21. Reference codes that start with a # (number sign).

Reference code	Description/Action
# followed by numbers, for example: #2533902	See Reference codes that begin with a number sign  . The information in this topic is intended for service providers.

HMC error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

Use this information to determine what a specific error or information message means and the recovery action, if applicable, to help you determine a recovery strategy.

Note: This is not a complete list of all the HMC error codes you might receive. If the code begins with ACT, HSCW, or HSCU, contact your next level of support or your service provider for more information.

0xxxxx connection error codes

If the HMC displays a state of No Connection in the managed system state column, it means that the HMC is unable to establish a connection to the managed system. There are several reasons why the HMC fails to establish connection, and often it is due to network issues. It is important to first check the network setting on both the HMC and the managed system. However, there are times a no connection state is caused by another problem unrelated to network settings. Use the following tables to find the error code you are receiving, and the recovery action if available.

Choose the range from the list below:

- 0x00xx
- 0x01xx
- 0x02xx
- 0x04xx
- 0x08xx
- 0x0Bxx
- 0x10xx

Range 0x00xx: Connection related failures during runtime (after initial command sequencing is complete)

0x00xx error codes (hex)	Text displayed	Recovery action
0x0000	Connecting	
0x0001	Connecting	<ol style="list-style-type: none"> 1. If the HMC does not recover automatically within a few minutes, do the procedure in Resetting the managed system connection from the HMC. 2. If the managed system is still showing No Connection on the HMC, contact your next level of support or your hardware service provider.
0x0002	Connecting	<ol style="list-style-type: none"> 1. If the HMC does not recover automatically within a few minutes, do the procedure in Resetting the managed system connection from the HMC. 2. If the managed system is still showing No Connection on the HMC, contact your next level of support or your hardware service provider.

0x00xx error codes (hex)	Text displayed	Recovery action
0x0003	Connecting	A reset connection of the managed system was initiated on the HMC. If the HMC does not recover automatically within a few minutes, contact your next level of support or your hardware service provider. Note: The managed system should not stay in this state for long. The HMC will re-establish connection to the system, and change to another state.
0x0004	Temporary disconnection	
0x0005	Permanent disconnection	
0x0006	Forced disconnection	If you no longer want your server to be HMC-managed, you must reset the server to a nonpartitioned server before removing the HMC. See Resetting the server to a nonpartitioned configuration for details.
0x0007	Connecting	<ol style="list-style-type: none"> 1. If the HMC does not recover automatically within a few minutes, do the procedure in Resetting the managed system connection from the HMC. 2. If the managed system is still showing No Connection on the HMC, contact your next level of support or your hardware service provider.
0x0008	Duplicate IP	<ol style="list-style-type: none"> 1. There is another managed system with the same IP address. Check whether there is an IP conflict. See Check for IP conflict. 2. Reset the managed system connection from the HMC. See Resetting the managed system connection from the HMC for details. 3. If the managed system is still showing No Connection on the HMC, contact your next level of support or your hardware service provider.
0x00FF	Connecting	<ol style="list-style-type: none"> 1. Reset the managed system connection from the HMC. See Resetting the managed system connection from the HMC for details. 2. If the managed system is still showing No Connection on the HMC, contact your next level of support or your hardware service provider.

Range 0x01xx: Socket-level connect failures

0x01xx error codes (hex)	Message	Recovery action
0x0101	DNS failure	<ol style="list-style-type: none"> 1. The HMC is unable to resolve the host name entered for the managed system through the domain name server. Check whether the DNS is down. 2. If the failure continues, remove the managed system connection and add it back using the IP address. Note: Leaving a connection in the DNS failed state might cause performance problems for other HMC connections.
0x0102	Connecting	The HMC is unable to establish a network connection to the managed system. Ensure that the managed system network is configured correctly.

0x01xx error codes (hex)	Message	Recovery action
0x0103	Connecting	<ol style="list-style-type: none"> 1. The target IP address of the managed system is refusing a connection from the HMC. Ensure that the IP specified is a valid managed system IP and that the managed system's network is configured correctly. 2. A connection might also be refused if the service processor firewall is configured to block this HMC IP address. Check the network configuration setting of your managed system to ensure that the HMC IP is not being blocked.
0x0104	IP unreachable	<ol style="list-style-type: none"> 1. The HMC is unable to establish a network connection to the managed system. Ensure the HMC and managed system are not on either side of a firewall, or if a firewall exists, ensure that the firewall is configured correctly. 2. Ensure that the managed system network is configured correctly. A common cause for this might be an invalid IP configuration on the HMC (for example, bad routing tables or default gateway).
0x01FF	Connecting	The HMC is unable to establish a network connection to the managed system. Ensure that the managed system network is configured correctly.

Range 0x02xx: SSL level connect failures

0x02xx error codes (hex)	Message	Recovery action
0x02FF	Connecting	<ol style="list-style-type: none"> 1. The HMC is unable to establish a secure network connection to the managed system. Reset the connection from the HMC. See Resetting the managed system connection from the HMC for details. 2. If the problem persists, contact your next level of support or your hardware service provider.

Range 0x04xx: Interface version related connection failures

0x04xx error codes (hex)	Message	Recovery action
0x0401	Interface version timed out	<ol style="list-style-type: none"> 1. If the HMC does not recover automatically within a few minutes, do the procedure in Resetting the managed system connection from the HMC. 2. If the managed system is still showing No Connection on the HMC, contact your next level of support or your hardware service provider.

0x04xx error codes (hex)	Message	Recovery action
0x0402	Already connected	<ol style="list-style-type: none"> 1. The managed system already has a connection established from the same HMC. If the HMC does not recover automatically within a few minutes, do the procedure in Resetting the managed system connection from the HMC. 2. If the managed system is still showing No Connection, then restart the HMC. 3. If the problem persists, contact your next level of support or your hardware service provider.
0x0403	All connections in use	<p>All connections available for HMCs are already in use. Determine what other HMCs are connected to the managed system, and remove the managed system connections from the other HMCs.</p> <p>Note: Contact your administrator to find out which HMCs can connect to the managed system.</p>
0x0404	Version mismatch	This version of HMC is unable to manage the system. Update the HMC image.
0x0405	Duplicate MTMS	There is already a managed system with the same machine type, model, and serial number. Contact your next level of support or your hardware service provider.
0x0406	Firmware not ready	<ol style="list-style-type: none"> 1. If the HMC does not recover automatically within a few minutes, do the procedure in Resetting the managed system connection from the HMC. 2. If the managed system is still showing No Connection on the HMC, contact your next level of support or your hardware service provider.
0x04FF	Connecting	<ol style="list-style-type: none"> 1. If the HMC does not recover automatically within a few minutes, do the procedure in Resetting the managed system connection from the HMC. 2. If the managed system is still showing No Connection on the HMC, your hardware service provider.

Range 0x08xx: Authentication related connection failures

0x08xx error codex (hex)	Message	Recovery action
0x0801	Authentication timed out	<ol style="list-style-type: none"> 1. Reset the managed system connection from the HMC. See Resetting the managed system connection from the HMC for details. 2. If the managed system is still showing No Connection on the HMC, contact your next level of support or your hardware service provider.
0x0802	Incorrect password	The password entered for the managed system is not correct. Check with your administrator to ensure that the password is correct and update the managed system password that the HMC is sending to the managed system. See Overview of the passwords for details.

0x08xx error codex (hex)	Message	Recovery action
0x0803	Firmware password locked	<ol style="list-style-type: none"> 1. There have been too many unsuccessful login attempts to the same managed system and the password is locked. Wait for five minutes, and reset the connection from the HMC. See Resetting the managed system connection from the HMC. 2. If the problem persists, contact your next level of support or your hardware service provider.
0x08FF	Connecting.	<ol style="list-style-type: none"> 1. If the HMC does not recover automatically within a few minutes, reset the managed system connection from the HMC. See Resetting the managed system connection from the HMC. 2. If the managed system is still showing No Connection on the HMC, contact your next level of support or your hardware service provider.

Range 0x0Bxx: Password change pending related connection failures

0x0Bxx error codes (hex)	Message	Recovery action
0x0BFF	Connecting.	<ol style="list-style-type: none"> 1. If the HMC does not recover automatically within a few minutes, reset the managed system connection from the HMC. See Resetting the managed system connection from the HMC. 2. If the managed system is still showing No Connection on the HMC, contact your next level of support or your hardware service provider.

Range 0x10xx: Get interface implementation limits related connection failures

0x10xx error codes (hex)	Message	Recovery action
0x1001	Command timed out.	<ol style="list-style-type: none"> 1. If the HMC does not recover automatically within a few minutes, reset the managed system connection from the HMC. See Resetting the managed system connection from the HMC. 2. If the managed system is still showing No Connection on the HMC, contact your next level of support or your hardware service provider.
0x10FF	Connecting	<ol style="list-style-type: none"> 1. If the HMC does not recover automatically within a few minutes, reset the managed system connection from the HMC. See Resetting the managed system connection from the HMC. 2. If the managed system is still showing No Connection on the HMC, contact your next level of support or your hardware service provider.

ESA0xxxx Electronic Service Agent error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

ESA0xxx error codes	Message	Recovery action
ESA00001	You must enter a valid IBM ID.	
ESA00002	Issuing authorization request for the following IBM IDs: {0}	
ESA00003	Issuing authorization request for the following IBM ID's: {0}{1}	
ESA00004	Your Hardware Management Console is not currently configured for remote service. Ensure that this Hardware Management Console is configured for remote service under Remote Support.	See "Enabling remote support on the HMC" on page 103.
ESA00005	The application can not currently find access to a call home server. Ensure that one of your Hardware Management Console's is configured as a call home server under Remote Support.	See "Enabling remote support on the HMC" on page 103.
ESA00006	Your Hardware Management Console is not currently configured for remote service and can not currently find access to a call home server. Ensure that this Hardware Management Console is configured for remote service and that one of your Hardware Management Console's is configured as a call home server under Remote Support.	See "Enabling remote support on the HMC" on page 103.
ESA00007	Remote Support is not currently supported on this Hardware Management Console.	
ESA00008	A request to authorize users was successfully created.	
ESA00009	An attempt to create an authorize users request was unsuccessful.	
ESA0000A	You must select an email address to perform the desired operation.	
ESA0000B	Successfully removed the following email addresses: {0}	
ESA0000C	Successfully sent email to the following addresses: {0}	
ESA0000D	Transmit of email request was unsuccessful. Ensure that the SMTP server and Port number specified are correct.	
ESA0000E	A request to transmit service information has been successfully created. Once the data has been gathered it will be transmitted.	

ESA0xxxx error codes	Message	Recovery action
ESA0000F	Successfully updated the frequency and time when the scheduled transmission of service information will occur.	
ESA00010	Successfully updated settings.	
ESA00011	Unsuccessfully sent email to the following addresses: {0} Ensure that the email address(s) is specified correctly and retry the operation.	
ESA00012	When you enable email notification, you must specify both an SMTP server and port number.	
ESA00013	A request to transmit performance management information has been successfully created. Once the data has been gathered it will be transmitted.	

HSCExxxx console events error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

HSCExxxx error codes	Message	Recovery action
HSCE2066	A scheduled backup of critical console data failed with a return code of {0}.	<p>The possible return code values are:</p> <ul style="list-style-type: none"> • A 4 indicates that the removable media could not be mounted. Verify that the media is inserted correctly in the drive and try the operation again. • A 5 indicates that the removable media is write protected. Remove write protection and try the operation again. • Any value except 4 or 5 is an internal HMC error. Perform the procedure in Backing up critical HMC data. If the problem persists, contact your next level of support or your service provider.

HSCFxxxx Licensed Internal Code error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

HSCFxxxx error codes	Message	Recovery action
HSCF0001	Select at least one Licensed Internal Code type to be updated.	
HSCF0002	Flash side selected for next activation: t-side	No recovery action is needed.

HSCFxxxx error codes	Message	Recovery action
HSCF0003	Flash side selected for next activation: p-side Attention: Selecting p-side for next activation will disable concurrent LIC update. The selection is for the next activation. To make it the currently active side, the target must be activated.	To switch to the temporary side, refer to “Working with the temporary and permanent side of the service processor” on page 208.
HSCF0004	An error occurred trying to survey the target {0}. The task will be terminated.	
HSCF0005	Managed System and Power LIC is selected for updating, but no target is currently selected. Ensure that the Managed System and Power LIC checkbox is not checked, or click Advanced Options to select a target.	
HSCF0006	I/O LIC is selected for updating, but no device is currently selected. Ensure that the I/O LIC checkbox is not checked, or click Advanced Options to select a device.	
HSCF0007	An error was encountered while reconfiguring the target {0} for updating through the Hardware Management Console. The selected action can not be performed at this time.	
HSCF0008	The selected installation type indicates to install and activate concurrently, but one or more selected targets have a disruptive concurrency status. Either select a different installation type, or ensure there are no targets selected with a concurrency status of “All must be disruptively activated.”	
HSCF0009	Failure importing the following I/O microcode {0}	
HSCF0010	I/O level details are not available.	
HSCF0011	Select a row in the table, and try the operation again.	
HSCF0012	Permanent flash side is active.	To switch to the temporary side, refer to “Working with the temporary and permanent side of the service processor” on page 208.
HSCF0013	There are no applicable levels for displaying cover letter information.	

HSCFxxxx error codes	Message	Recovery action
HSCF0014	At least one target has its flash p-side active. Contact a user with service mode authority to use the Flash Side Selection task to make the flash t-side active, and then start this task again. The affected target(s): {0}.	To switch to the temporary side, refer to “Working with the temporary and permanent side of the service processor” on page 208.
HSCF0015	An internal code error occurred on the target {0}. The task will be terminated	
HSCF0016	The operation failed because the drive is in use or can not be accessed for some other reason.	
HSCF0017	The DVD does not contain any applicable upgrade updates. Insert another DVD, and click {0}.	
HSCF0018	At least one target does not have an applicable upgrade update. Start the task again without selecting the following target(s): {0}.	
HSCF0019	Retrieving updates.	
HSCF0020	Installing updates.	
HSCF0021	Activating updates - Power Off.	
HSCF0022	Activating updates - Restarting FSP.	
HSCF0023	Activating updates - Power On.	
HSCF0024	Activating updates - FSP.	
HSCF0025	Activating updates - PHYP.	
HSCF0026	Activating updates - PFW.	
HSCF0027	Update complete.	
HSCF0028	Removing updates.	
HSCF0029	Saving accepted level.	
HSCF0030	Saving accepted level.	
HSCF0031	Unable to contact the IBM service web site.	
HSCF0032	Unable to contact the IBM support system.	
HSCF0033	Unable to contact the FTP site.	
HSCF0034	Unable to log into the FTP site using the specified user ID and password.	
HSCF0035	Unable to access the specified FTP site directory.	
HSCF0036	The connection to the target was lost during a reboot of the FSP.	
HSCF0037	Licensed Internal code was changed as requested, but a failure occurred returning the managed system to its original state.	

HSCFxxxx error codes	Message	Recovery action
HSCF0038	Retrieve of licensed internal code failed.	
HSCF0039	{0} of {1} FRUs updated during phase {2} of power ACDL on {3}	
HSCF0040	Power ACDL started on {0}.	
HSCF0041	Licensed Internal Code update cannot be started because ACDL is pending on {0}.	
HSCF0042	Licensed Internal Code update cannot be started because {0} has N mode power.	<p>The system has power to only one of the two AC power cords.</p> <p>In general, N mode power means the system is not operating in a redundant state (N+1 power means the system can survive the loss of that particular power component).</p> <p>If both line cords are not powered, only one Bulk Power Controller (BPC) will be powered. Both BPCs need to be powered to load LIC.</p>
HSCF0043	<p>The installation type for Managed System and Power LIC indicates to install and activate disruptively. I/O LIC cannot be updated when that installation type is selected.</p> <p>Ensure that either the I/O LIC checkbox is not checked, or click the Back button and ensure that the Managed System and Power LIC checkbox is not checked. When the LIC update completes, you can restart the Change Internal Code wizard to install the other LIC updates.</p>	
HSCF0044	Select a single row in the table, and try the operation again.	
HSCF0045	Firmware update was successful to all primary service processors for the targeted object. There was a failure attempting to update the backup service processor for {0}.	
HSCF0046	Firmware update was successful to all primary service processors for the targeted object. There was a failure attempting to update I/O microcode on {0}.	
HSCF0047	This message was used temporarily in a previous release only.	
HSCF0048	Power code download failed.	
HSCF0049	Failure downloading file {0} from the IBM service web site.	
HSCF0050	The repository does not contain any applicable upgrade updates.	

HSCF _{xxxx} error codes	Message	Recovery action
HSCF0051	There is a new upgrade release available at the repository.	
HSCF0052W	The frame is locked by another process and cannot run another process.	To clear this condition, run the <code>rmlock -e</code> command from the HMC command line. For example, <code>rmlock -e 9458-100*918002M</code> .
HSCF0071E	Communication error to Side A B BPC on <code>tttt-mmm*sssssss</code> : No connection exists.	There is no connection data found for the Bulk Power Controller.
HSCF0071E	Communication error to Side A B BPC on <code>tttt-mmm*sssssss</code> : Surveillance command failed.	<ol style="list-style-type: none"> 1. Correct any open issues in the Service Focal Point. For details see "Using Service Focal Point for the HMC" on page 436. 2. Retry the Licensed Internal Code update. 3. If the problem persists, contact your next level of support.
HSCF0071E	Communication error to Primary Secondary FSP on <code>tttt-mmm*sssssss</code> : No connection exists.	<ol style="list-style-type: none"> 1. Correct any open issues in the Service Focal Point. For details see "Using Service Focal Point for the HMC" on page 436. 2. Retry the Licensed Internal Code update. 3. If the problem persists, contact your next level of support.
HSCF0071E	Communication error to Primary Secondary FSP on <code>tttt-mmm*sssssss</code> : Surveillance command failed.	<ol style="list-style-type: none"> 1. Correct any open issues in the Service Focal Point. For details see "Using Service Focal Point for the HMC" on page 436. 2. Retry the Licensed Internal Code update. 3. If the problem persists, contact your next level of support.
HSCF0079E	Managed system state <i>state</i> on <code>ttt-mmmm*sssssss</code> is incorrect. Valid states are: Operating, Power Off, Error – Terminated, Standby.	<ol style="list-style-type: none"> 1. Correct the managed system operating state. For details see "Correcting the managed system operating state" on page 428. 2. Retry the Licensed Internal Code update. 3. If the problem persists, contact your next level of support.
HSCF0080E	Side A B BPC on <code>tttt-mmm*sssssss</code> has failed a redundancy test.	<ol style="list-style-type: none"> 1. Correct any open issues in the Service Focal Point. For details see "Using Service Focal Point for the HMC" on page 436. 2. Retry the Licensed Internal Code update. 3. If the problem persists, contact your next level of support.
HSCF0081E	ACDL is pending for Side A B BPC on <code>tttt-mmm*sssssss</code> .	<ol style="list-style-type: none"> 1. Correct any open issues in the Service Focal Point. For details see "Using Service Focal Point for the HMC" on page 436. 2. Retry the Licensed Internal Code update. 3. If the problem persists, contact your next level of support.

HSCFxxxx error codes	Message	Recovery action
HSCF0082E	<p>Side A B BPC on tttt-mm*sssssss has reported an error condition: reason.</p> <p>Reason could be one of the following:</p> <p>Fault indicator is true</p> <p>All Good indicator is false</p> <p>Mailbox Present indicator is false</p> <p>BPF Good indicator is false</p>	<ol style="list-style-type: none"> 1. Correct any open issues in the Service Focal Point. For details see "Using Service Focal Point for the HMC" on page 436. 2. Retry the Licensed Internal Code update. 3. If the problem persists, contact your next level of support.
HSCF0083E	<p>Primary FSP on tttt-mm*sssssss has reported an error condition: reason.</p> <p>Reason could be one of the following:</p> <p>Secondary FSP is not functional</p> <p>Secondary FSP is guarded</p>	<ol style="list-style-type: none"> 1. Correct any open issues in the Service Focal Point. For details see "Using Service Focal Point for the HMC" on page 436. 2. Retry the Licensed Internal Code update. 3. If the problem persists, contact your next level of support.

HSCIxxxx Inventory Scout Services error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

HSCIxxxx error codes	Message	Recovery action
HSCI0100	No managed systems were detected that are attached to this system console.	
HSC0101	No logical partitions have been defined for this managed system.	
HSC0102	A blank or invalid entry was entered in the partition password field.	Enter a valid password value.
HSC0103	A blank or invalid entry was entered in the listening port field.	Enter a valid port value.
HSC0104	A blank or invalid entry was entered in the IP address field.	Enter a valid IP address value.
HSC0110	The Inventory Scout Services command completed successfully.	
HSC0111	The Inventory Scout Services command request failed	<ol style="list-style-type: none"> 1. Verify that the removable media is correctly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. Contact your next level of support or your service provider.

HSCIxxx error codes	Message	Recovery action
HSC0112	The removable media cannot be mounted. Ensure the media is inserted correctly in the drive and retry the operation.	<ol style="list-style-type: none"> 1. Verify that the removable media is correctly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. Contact your next level of support or your service provider.
HSC0113	The media specified is write protected. Adjust the media and retry.	Remove write protection and try the operation again.
HSC0114	The Inventory Scout Services request failed. Ensure the removable media is correctly inserted in the drive.	<ol style="list-style-type: none"> 1. Verify that the removable media is correctly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. Contact your next level of support or your service provider.
HSC0115	An error occurred while copying the Inventory Scout Services data. Verify that a blank formatted diskette is inserted correctly in the drive and retry the operation.	<ol style="list-style-type: none"> 1. Verify that the removable media is correctly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. Contact your next level of support or your service provider.
HSC0116	An error occurred while compressing the Inventory Scout Services data. Retry the operation.	<ol style="list-style-type: none"> 1. Verify that the removable media is correctly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. Contact your next level of support or your service provider.
HSC0117	An error occurred while trying to unmount the media.	<ol style="list-style-type: none"> 1. Verify that the removable media is correctly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. Contact your next level of support or your service provider.
HSC0118	The Inventory Scout Services daemon was restarted successfully.	
HSC0119	The Inventory Scout Services daemon could not be restarted.	<ol style="list-style-type: none"> 1. Verify that the removable media is correctly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware to determine if there is a hardware problem. 4. Contact your next level of support or your service provider.

HSCIxxx error codes	Message	Recovery action
HSC0120	The internal managed system name is malformed. Exit this task and retry the operation.	<ol style="list-style-type: none"> 1. Verify that the removable media is correctly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor. 4. Contact your next level of support or your service provider.
HSC0121	The Inventory Scout Services request failed. An error occurred while copying data to removable media.	<ol style="list-style-type: none"> 1. Verify that the removable media is correctly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. Contact your next level of support or your service provider.

HSClxxxx error codes	Message	Recovery action
HSC0122	The system partitions did not respond to query attempts.	<ol style="list-style-type: none"> 1. Check that the HMC host name and the host name of the partition are fully qualified domain names (not a short host name). If they are not, this must be corrected for remote security to work. 2. Verify that the network routing is set up so the HMC can use ping to reach the partition and vice versa. If one or both cannot be reached from the other, correct the routing. 3. Ensure that <code>/var</code> is not full on the partition, which would prevent certain processes from running correctly. 4. Verify that the following file sets have been installed correctly on the AIX logical partitions: <ul style="list-style-type: none"> • <code>rsct.core</code> • <code>csm.client</code> • <code>devices.chrp.base.ServiceRM</code> 5. Log in to one of the logical partitions and issue the following command: <code>lssrc -s ctcas</code> 6. If the output shows <code>ctcasd</code> is inoperative, issue the command: <code>ls -l</code> on the <code>/var/ct/cfg/</code> directory. 7. If the files <code>ct_has.pkf</code> and <code>ct_has.qkf</code> are zero-length, there was an (AIX) installation configuration problem. These zero-length files should be removed. 8. Issue the command <code>startsrc -s ctcas</code> If the <code>startsrc -s ctcas</code> command does not work, the AIX lpp might not have been installed. 9. If the output is still blank, shut down and restart the HMC. 10. After the shutdown and restart occurs, wait at least 10 minutes before trying again to ensure all the logical partitions have resynchronized their information with the HMC. 11. If the problem persists, contact your next level of support or your service provider.

HSCLxxxx error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

The HSCL error codes in this list are organized by their first character, with numbers coming before letters.

00xx	06xx	11xx	24xx	90xx
01xx	07xx	13xx	25xx	Axxx
02xx	09xx	14xx	29xx	

03xx	0Bxx	15xx	3xxx
04xx	0Dxx	17xx	70xx
05xx	0Fxx	19xx	80xx

HSCL00xx Profile data error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCL00xx error codes	Message	Recovery action
HSCL0003	The profile data save area is full. Remove any profiles that are no longer needed.	Remove the profiles that are no longer needed.
HSCL0004	A profile with name {0} already exists in the partition with ID {1} in the profile data of the managed system. Provide another name for this profile.	Rename the profile to a name that is not already in use in this partition.
HSCL0005	Cannot find information regarding profile data of the managed system. Run a rebuild managed system operation.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0006	The managed system's profile data has been corrupted. You must either restore or reinitialize the profile data.	<ol style="list-style-type: none"> 1. Restore the profile data. For details, see Recovering partition data on a managed system. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0007	The profile data of the managed system cannot be accessed or modified. Run a rebuild managed system operation.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0008	Could not construct or initialize profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0009	Could not construct or initialize the profile data from the backup file, {0}. Repeat the operation.	<ol style="list-style-type: none"> 1. Repeat the operation. 2. If the problem persists, see Recovering partition data on a managed system. 3. If the problem persists, contact your next level of support or your service provider.
HSCL000A	Could not build the profile for the managed system. Repeat the operation.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL000B	Could not get the activated partition profile from the profile data. Perform a rebuild managed system operation.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.

HSCL00xx error codes	Message	Recovery action
HSCL000C	Could not get the activated system profile from the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL000D	Could not get all the system profiles from the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL000E	Could not get the default system profile from the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL000F	Could not get the default system profile from the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0010	Could not get the partition profile from the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0011	Could not get the partition profiles for the partition from the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0012	Could not get the system profile from the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0013	Could not remove the partition profile from the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0014	Could not remove the system profile from the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0015	Could not save the LPAR profile to the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0016	Could not save the system profile to the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.

HSCL00xx error codes	Message	Recovery action
HSCL0017	Could not create the partition profile in the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0018	Could not create the system profile in the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0019	Could not set the activated partition profile in the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL001A	Could not set the activated system profile in the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL001B	Could not set the default partition profile in the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL001C	Could not set the default system profile in the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL001D	Could not clean up the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL001E	Could not update the profile data cache. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL001F	Could not check for duplicate partition name. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0020	Could not remove the partition profile from the system profile content in the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0021	Could not add the partition profile to the system profile in the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.

HSCL00xx error codes	Message	Recovery action
HSCL0022	Could not get the partition name from the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0023	Could not get all the partition names from the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0024	Could not set the partition name in the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0025	Could not build the profile data from the local file, {0}. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0026	Could not write the data to the managed system. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0027	Could not back up the profile data to a file. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0028	Could not read profile data from the managed system. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0029	Could not delete profiles at the partition with ID of {0} in the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL002A	Could not modify the system profiles containing the LPAR slot ID of {0} in the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL002B	Could not perform a priority restore on the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL002C	Could not merge the profile information in the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.

HSCL00xx error codes	Message	Recovery action
HSCL002D	Could not merge partition name data in the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL002E	Could not merge default and activated list data in the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0030	Could not initialize the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0031	The profile data has been cleared. Either restore or reinitialize the profile data save area.	<ol style="list-style-type: none"> 1. Restore the profile data. For details, see Recovering partition data on a managed system. 2. If the problem persists, contact your next level of support or your service
HSCL0032	Could not set the system profile's user-defined name to the profile data. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0033	This managed system version, {0}, is unknown to HMC. Update to an HMC release that can handle this version of managed system.	<ol style="list-style-type: none"> 1. Rebuild managed system. For details, see Updating managed system or frame information for details. 2. If the same error occurs, update to an HMC release that can handle this version of managed system. 3. If you are not sure what version to use, contact your next level of support or your service provider.
HSCL0034	The levels of managed system and profile data area are not matching. Managed system version: {0}, profile data area version: {1}. Upgrade the managed system version to the correct level.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information for details. 2. If the same error occurs, update the managed system to a correct version. 3. If you are not sure what version to use, contact your next level of support or your service provider.
HSCL0035	Cannot restore profile data with two different versions of profile save data.	<ol style="list-style-type: none"> 1. Perform the operation again. 2. If the same error occurs, restore using another profile data file. For details, see Recovering partition data on a managed system. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0036	Migrate profile data failed.	<ol style="list-style-type: none"> 1. Perform the operation again. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0037	This level of profile data, {0}, is unknown to this HMC. Update to an HMC version that can handle this level of profile data.	<ol style="list-style-type: none"> 1. Perform the operation again. 2. If the problem persists, update to an HMC version that can handle this level of profile data. 3. If you are not sure what version to use, contact your next level of support or your service provider.

HSCL00xx error codes	Message	Recovery action
HSCL0038	Creation of logical partition profiles failed in the profile data save area.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information for details. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0039	Deletion of logical partitions failed in the profile data save area.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information for details. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL003A	Removal of system profiles failed at profile data save area.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information for details. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL003B	Setting of partition information failed in the profile data save area.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL003C	Retrieval of all logical partition information failed in the profile data save area.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information for details. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL003D	Retrieval of partition information failed in the profile data save area.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information for details. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0041	Migration of partition information failed in the profile data save area.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information for details. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0042	Migration of profile names failed in the profile data save area.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information for details. 2. If the problem persists, contact your next level of support or your service provider.

HSCL00xx error codes	Message	Recovery action
HSCL0043	Migration of default profile list failed in the profile data save area.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information for details. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0044	Migration of activated profile list failed in the profile data save area.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information for details. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0046	Migration of I/O unit and profile information failed in the profile data save area.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information for details. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0047	Migration of time stamps of profile data save area failed.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information for details. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0048	Migration of checksums of the profile data save area failed.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information for details. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0049	Unable to get next available profile ID from the HMC profile data.	
HSCL004A	HMC Save Area Set Fast Activation failed.	
HSCL004B	HMC Save Area Get Fast Activation failed.	
HSCL004C	Unable to open the HMC Save Area file.	
HSCL004D	The HMC could not retrieve information from the managed system.	
HSCL004E	Unable to set partition information in the profile data. Execute a rebuild managed system operation.	
HSCL004F	HMC Save Area Get System Credential Information failed.	
HSCL0050	HMC Save Area Set System Credential Information failed.	
HSCL0051	Cannot retrieve virtual Ethernet MAC address prefix.	<ol style="list-style-type: none"> 1. Try the operation again. 2. If the problem persists, contact your next level of support or your service provider.

HSCL00xx error codes	Message	Recovery action
HSCL0052	Cannot set virtual Ethernet MAC address prefix.	<ol style="list-style-type: none"> 1. Try the operation again. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0053	Attempt to update profile information failed due to invalid resource lock type.	<ol style="list-style-type: none"> 1. Try the operation again. 2. If the problem persists, contact your next level of support or your service provider.

HSCL01xx managed system error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCL01xx error codes	Message	Recovery action
HSCL01F7	Unable to get the current time from the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Try the task again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL01F8	This property cannot be altered.	
HSCL01F9	Could not create managed system instance in object manager.	<ol style="list-style-type: none"> 1. Try the task again. 2. Shut down and restart the HMC. For details, see Shutting down, rebooting, and logging of the HMC. 3. Try the task again.
HSCL01FA	The managed system is already powered off.	The managed system was already powered off before your attempt to power it off. No action is required.
HSCL01FB	The number of parameters is incorrect. Specify a different value.	
HSCL01FC	The parameter specified is not valid. Specify a different value.	
HSCL01FD	Power on failed. Try again.	<ol style="list-style-type: none"> 1. Retry starting the managed system. 2. If the problem persists, contact your next level of support or your service provider.
HSCL01FE	The managed system is already powered on.	

HSCL01xx error codes	Message	Recovery action
HSCL01FF	Could not rebuild. Shut down and restart the Hardware Management Console.	<ol style="list-style-type: none"> 1. Retry the task. 2. If it fails again, shut down and restart the HMC. For details, see Shutting down, rebooting, and logging of the HMC. 3. Check the state of the managed system. Refer to “Correcting the managed system operating state” on page 428 and perform the appropriate procedure to put the managed system in the correct state. 4. Try the task again. 5. If the problem persists, contact your next level of support or your service provider.

HSCL02xx error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCL02xx error codes	Message	Recovery action
HSCL0201	Service processor command failed after {0} attempts: Invalid response.	Wait several minutes and try the task again.
HSCL0203	Command sent to service processor failed. Error response {0}.	<ol style="list-style-type: none"> 1. Try the task again. 2. Check the state of the managed system. Refer to “Correcting the managed system operating state” on page 428 and perform the appropriate procedure to put the managed system in the correct state. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0204	Command failed. Unknown error.	<ol style="list-style-type: none"> 1. Shut down and restart the HMC. For details, see Shutting down, rebooting, and logging of the HMC. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0205	The managed system is in the error state and is unable to continue with the task.	<p>The recovery partition data task cannot be run until the managed system is no longer in error state.</p> <ol style="list-style-type: none"> 1. Record the error message. 2. Check the state of the managed system. Refer to “Correcting the managed system operating state” on page 428 and perform the appropriate procedure to put the managed system in the correct state.

HSCL02xx error codes	Message	Recovery action
HSCL0206	Unable to power on the managed system. Unable to continue with the power on task.	<ol style="list-style-type: none"> 1. Check the Operator panel value column for the managed system to verify that it is in the No power state and that the managed system is not in the Error state. 2. If the managed system is in the error state, refer to "Correcting the managed system operating state" on page 428 and perform the appropriate procedure to put the managed system in the correct state. 3. Verify that no other task is being performed, and then retry the task. 4. If the problem persists, contact your next level of support or your service provider.
HSCL0208	Unable to power on the managed system. Unable to continue with the power on task.	<ol style="list-style-type: none"> 1. Check the Operator panel value column of the managed system to verify that it is in the No power state and that the managed system is not in the Error state. 2. If the managed system is in the error state, refer to "Correcting the managed system operating state" on page 428 and perform the appropriate procedure to put the managed system in the correct state. 3. Verify that no other task is being performed while processing this task, and then retry the task. 4. If the problem persists, contact your next level of support or your service provider.
HSCL0209	Remote virtual terminal sessions are not allowed. Check the remote virtual terminal settings.	Virtual terminal cannot open remotely at this time. If this feature is needed, use the Enable/Disable Remote Virtual Terminal task in the HMC Configuration menu to enable remote connections.
HSCL020A	The power on system profile operation timed out. Activate the system profile manually after the managed system is powered on.	Activate the system profile manually after the managed system is powered on.
HSCL020D	The command you issued contained incorrect data.	Contact your next level of support or your service provider.
HSCL0211	The requested function is currently disabled.	Shut down the managed system, and start it again.
HSCL0212	The managed system is not capable of Capacity on Demand (CoD) at the present time.	<ol style="list-style-type: none"> 1. Ensure that the managed system is powered on. 2. If it is powered on, check the managed system's properties window to verify that the system is <i>not</i> CoD capable. 3. Contact your local representative for more information about this feature.
HSCL0213	The managed system does not support Capacity on Demand upgrades for processors.	Contact your local representative for more information about this feature.
HSCL0214	The managed system does not support Capacity on Demand upgrades for memory.	Contact your local representative for more information about this feature.
HSCL0215	There was an error trying to save processor order information to a diskette.	Verify that the diskette is writable, and retry the operation again. If the error persists, contact your next level of support or your service provider.

HSCL02xx error codes	Message	Recovery action
HSCL0222	The operation cannot be done because the managed system is not capable of LPAR.	<ol style="list-style-type: none"> 1. If you believe that the managed system should be capable of logical partitioning, restart the HMC and retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0223	Firmware is not ready to accept the specified command. Try again later.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0224	There was an error dumping the LPAR configuration. Check the console event log.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0225	There was an error clearing the LPAR configuration. Check the console event log.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0226	The firmware power off policy returned from the service processor is not valid. Unable to determine whether the firmware should power off or stay running after last partition powers off.	<ol style="list-style-type: none"> 1. Check that the inputs are correct. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0228	The managed system could not be found in the database. Rebuild the managed system, and try again.	<ol style="list-style-type: none"> 1. Shut down and restart the HMC. 2. Rebuild the managed system. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0229	Memory specified, {0}, is not a multiple of the system memory region size, {1}. Modify the value to be a multiple of the memory region size and try again.	<ol style="list-style-type: none"> 1. Modify the value of the memory specified to be a multiple of the memory region size and try the operation again. 2. If the problem persists, contact your next level of support or your service provider.
HSCL022A	i5/OS partitions are not supported on the managed system.	<ol style="list-style-type: none"> 1. The managed system is not capable of creating or managing i5/OS partitions. 2. If you believe that the managed system should be i5/OS capable, restart the HMC and retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL022C	The managed system is not in a valid state to perform the operation. Check the state of the managed system and retry the operation.	<ol style="list-style-type: none"> 1. Try the task again. 2. Refer to “Correcting the managed system operating state” on page 428 and perform the appropriate procedure to put the managed system in the correct state. 3. If the problem persists, contact your next level of support or your service provider.

HSCL02xx error codes	Message	Recovery action
HSCL022D	Unable to perform a get or a set operation on the managed system's platform IPL parameters.	<ol style="list-style-type: none"> 1. Try the task again. 2. Perform the appropriate actions to put the managed system in the correct state. For details, see "Correcting the managed system operating state" on page 428. 3. If the problem persists, contact your next level of support or your service provider.
HSCL022E	Unable to restore the profile data when the managed system is not in the Operating or Standby state.	<ol style="list-style-type: none"> 1. Verify that the managed system is in the Operating or Standby state, and retry the operation. 2. If the managed system is not in the correct state, refer to "Correcting the managed system operating state" on page 428 and perform the appropriate procedure to put the managed system in the correct state. 3. If the problem persists, contact your next level of support or your service provider.
HSCL022F	Unable to delete the profile data backup file, {0}.	<ol style="list-style-type: none"> 1. Try the task again. 2. Rebuild the managed system and try the task again. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0230	Unable to get managed system credential information.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. Then try the task again. 2. Restart the HMC and then retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0231	Unable to set managed system credential information.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. Then try the task again. 2. Restart the HMC and then retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0233	Unable to change the service partition to the partition with ID of {0}. Check your current setting(s) and ensure this change is allowed.	<p>The service partition cannot be changed.</p> <ol style="list-style-type: none"> 1. Check current settings and verify that this change is allowed. 2. Rebuild the managed system and try the operation again. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0234	Failed to transition out of standby state. Rebuild the managed system and try again.	<p>Rebuild the managed system. For details, see Updating managed system or frame information. Then try the task again.</p> <p>If the problem persists, contact your next level of support or your service provider.</p>

HSCL02xx error codes	Message	Recovery action
HSCL0235	Cannot change service partition from one partition to another if either one of them is not in the Not Activated state.	<ol style="list-style-type: none"> 1. Ensure that the current service partition is not activated. 2. Ensure that the partition user who tried to assign the server authority is not activated. 3. Rebuild the managed system. For details, see Updating managed system or frame information. Then try the task again. 4. If the problem persists, contact your next level of support or your service provider.
HSCL0236	The name specified contains unprintable or invalid characters listed: {0}. Remove the invalid characters and try again.	<ol style="list-style-type: none"> 1. Ensure that all the characters specified in the name are valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0240	The {0} password is locked and cannot be changed while it is locked.	The password has been locked. Contact your next level of support or your hardware service provider to unlock the password.
HSCL0241	The {0} password is locked.	The password has been locked. Contact your next level of support or your hardware service provider to unlock the password.
HSCL0242	Failed to set i5/OS partition {0} as the service partition for this managed system. Only an AIX or Linux logical partition can be designated as the service partition on IBM System p5 or IBM eServer p5 servers.	Choose an AIX or Linux logical partition as the service partition for your managed system.
HSCL0243	The Machine Code on your managed system does not support viewing the Virtualization Engine systems technologies activation history log. In order to view the history log on your managed system, you need to update your managed system's Machine Code (Licensed Internal Code).	<ol style="list-style-type: none"> 1. Contact your service provider to determine which level of HMC Machine Code supports viewing the Virtualization Engine systems technologies activation history log. 2. Update your managed system's Machine Code to that level or greater. For details, see "Obtaining updates" on page 121. 3. Try the task again.
HSCL0250	The managed system machine type, model, and serial number (MTMS) is empty.	
HSCL0251	Service processor command {0} failed. The connection to the hardware server is broken.	Ensure that the network connection is working. If the problem persists, contact your next level of support or your service provider.
HSCL0252	Service processor command {0} failed. The connection to service processor is not available.	Ensure that the network connection is working. If the problem persists, contact your next level of support or your service provider.
HSCL0253	Service processor command {0} failed. The managed system has been deleted.	Ensure that the network connection is working. If the problem persists, contact your next level of support or your service provider.
HSCL0254	Hardware server command {0} failed. No response package.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.

HSCL02xx error codes	Message	Recovery action
HSCL0255	Hardware server command {0} failed. The request ID has been deleted from the ID table.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0256	Issuing a service processor pass-through failed. HMC server is trying to reconnect to the hardware server.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0257	Issuing a service processor pass-through failed. HMC server re-established a connection to the hardware server after this command was issued.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0258	Issuing a service processor pass through failed. An expected exception with message {0} was thrown.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0259	Service processor lock failed. The lock manager is not active.	Restart the HMC. If the problem persists, contact your next level of support or your service provider.
HSCL025A	Service processor lock failed. The conflict lock is owned by HMC: {0}. Its request ID is {1}. Try again later.	<ol style="list-style-type: none"> 1. Another HMC might be performing this operation. 2. Try again later. 3. If the problem persists, contact your next level of support or your service provider.
HSCL025B	Query service processor data failed. The error code is {0}.	
HSCL025C	Service processor command {0} failed. Service processor authentication needs to be done first.	<ol style="list-style-type: none"> 1. Ensure that the managed system is authenticated first. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL025D	Service processor command {0} failed. The Hypervisor is not ready to accept commands.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information 2. If the problem persists, contact your next level of support or your service provider.
HSCL025E	The lock table in the managed system is full. Try again.	Wait and then try the operation again.
HSCL025F	There is a managed system lock.	Wait and then try the operation again.
HSCL0260	Unexpected error happened when trying to acquire a managed system lock. The command return status is {0}.	Wait and then try the operation again.
HSCL0261	Unexpected error happened when trying to acquire a managed system lock.	Report the problem to your next level of support or your service provider.
HSCL0262	Supplement lock operation failed.	Check the input and permission and try the task again.
HSCL0263	Service processor does not support more than one HMC connection. No service processor lock is needed.	contact your next level of support or your service provider.

HSCL02xx error codes	Message	Recovery action
HSCL0264	The console command manager is not active.	<ol style="list-style-type: none"> 1. Try the operation again. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0265	No destination was specified for command {0}. The command cannot be sent.	<ol style="list-style-type: none"> 1. Try the operation again. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0266	The request to query data on the managed system failed with error code {0}.	<ol style="list-style-type: none"> 1. Try the operation again. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0267	The connection to the service processor has been lost. A long-running task was stopped.	Verify the completion of the long-running task. If the task did not complete successfully, try the task again
HSCL0268	An unexpected error occurred in a long-running task.	Verify the completion of the long-running task. If the task did not complete successfully, try the task again.
HSCL0269	Managed system with IP address {0} cannot be found.	Verify the specified IP address. Specify a valid IP address and try the request again.
HSCL026A	The specified managed system name {0} is not valid with the specified IP address {1}. The managed system cannot be removed.	Specify a valid managed system name and a valid IP address. Then try the request again.
HSCL026B	Cannot find a managed system with the specified name {0}.	Verify the specified system name. Specify a valid managed system name and try the request again.
HSCL026C	The request to add a new managed system with IP address {0} failed.	Verify the specified IP address. Specify a valid IP address and try the request again.
HSCL026D	Lock type {0} is not valid for the managed system.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL026E	The lock manager for managed system {0} is not active.	Try the request again later. If the problem persists, contact your service provider.
HSCL026F	Either the managed system name or the IP address is not specified in the request to remove the managed system.	Specify both the managed system name and the IP address. Then try the request again.
HSCL0270	The specified command destination {0} cannot be found. The command {1} cannot be sent.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0271	The connection state of the specified command destination {0} is not valid. The command {1} cannot be sent.	The connection to the managed system has been lost. Try the request again later.
HSCL0280	The service processor managed system state is not valid. The power state is {0}. The run state is {1}.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0281	The operation cannot be done because the managed system is not shared processor capable.	No recovery action is required.

HSCL02xx error codes	Message	Recovery action
HSCL0282	The virtual Ethernet adapter in virtual I/O slot {0} cannot be defined because the partition with ID {1} already defines a trunk adapter in its virtual I/O slot {2}. Modify the profile accordingly and reactivate the partition.	Modify the profile accordingly and reactivate the partition.
HSCL0285	The managed system does not support SNI message passing.	No recovery action.
HSCL0288	The managed system is not ready for service processor failover.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL023A	This operation is allowed only when the managed system is powered off.	No recovery action.
HSCL023B	This operation is allowed only after the managed system has been powered on at least once, and then powered off.	No recovery action.

HSCL03xx managed system resource error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCL03xx error codes	Message	Recovery action
HSCL03EA	There is an insufficient number of processors: Obtained - {0}, Required - {1}. Check that there are enough processors available to activate the partition. If not, create a new profile or modify the existing profile with the available resources, and then activate the partition. If the partition must be activated with the specified number of processors, deactivate any active logical partitions using the resource, and then activate the partition.	<ol style="list-style-type: none"> 1. Check the managed system properties window to ensure that enough processors are available to activate the partition. 2. If there are not enough processors available, create a new profile or modify the existing profile with the available resources. Then activate the partition. 3. If the partition must be activated at any cost, deactivate any running partition that is using the resource and then activate the partition. 4. If the problem persists, contact your service provider.

HSCL03xx error codes	Message	Recovery action
HSCL03EB	Unable to allocate the I/O slot {0} for activation. This I/O slot is identified as a required adapter to activate this partition. Verify that the specified I/O is available to activate the partition. If it is not available, either create a new profile or modify the existing profile to identify the I/O adapter as a non-required resource, and then try to activate the partition again. If the partition must be activated with these resources, deactivate any running partition that is using the resource, and then try to activate this partition again.	<ol style="list-style-type: none"> 1. Check the managed system properties window to ensure that enough I/O slots are available to activate the partition. 2. If there are not enough I/O slots available, create a new profile or modify the existing profile with the available resources. Then activate the partition. 3. If the partition must be activated at any cost, deactivate any running partition that is using the resource and then activate the partition. Note: If you must activate the partition and you have tried unsuccessfully to recover using the above action, edit the profile for the partition you are activating and remove all slots that are associated with the identified slot's PHB. See the PCI Adapter Placement Reference, order number SA38-0538 for information on PHB slot associations. 4. If the problem persists, contact your service provider.
HSCL03EC	There is not enough memory: Obtained - {0}, Required - {1}. Check that there is enough memory available to activate the partition. If not, create a new profile or modify the existing profile with the available resources, then activate the partition. If the partition must be activated with these resources, deactivate any running partition or partitions using the resource, then activate this partition.	<ol style="list-style-type: none"> 1. Check the managed system properties window to ensure that enough memory is available to activate the partition. 2. If there is not enough available memory, create a new profile or modify the existing profile with the available resources and then activate the partition. 3. If the partition must be activated at any cost, deactivate any running partition using the resource, and activate the partition. 4. If the problem persists, contact your service provider.
HSCL03ED	The I/O unit specified by this ID cannot be found and might have been deleted from the managed system. Modify the profile.	Modify the partition profile so that the unit that cannot be found is no longer part of the profile's resources.
HSCL03EE	The specified slot number cannot be found. Ensure the profile is not using I/O unit slots that do not exist in the managed system.	The adapter specified cannot be found. Modify partition profiles so that the slot that cannot be found is not part of any partition profile.
HSCL03EF	The number of system units, slots, and I/O required and desired information stored in the properties do not match. The profile might be corrupted. Perform the Restore Profile Data task.	<ol style="list-style-type: none"> 1. The profile might be corrupted. Restore the profile data. For details, see Restoring profile data. 2. If the problem persists, delete the profile and create a new profile.
HSCL03F0	Could not allocate the I/O slot for activation in I/O drawer {0}. Slot {1} is currently being used by another partition. Perform one of the following three actions: 1) Remove this I/O slot from the profile, 2) Change the I/O slot from Required to Desired in the profile, or 3) Remove the I/O slot from the other partition.	<p>Perform one of the following actions:</p> <ul style="list-style-type: none"> • Remove this I/O slot from the profile. • Change the I/O slot from Required to Desired in the profile. • Remove the I/O slot from the other partition.

HSCL03xx error codes	Message	Recovery action
HSCL03F4	Not enough processing resources to meet the allocation setting	<ol style="list-style-type: none"> 1. Ensure there is enough processors to start the partition. 2. Rebuild the managed system. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL03F5	There is an insufficient amount of shared processing resources: Virtual processor obtained - {0}, processing units obtained - {1}, Required virtual processors - {2}, Required processing units - {3}. Check that there is enough processing resources available to activate the partition. If not, create a new profile or modify the existing profile with the available resources, then activate the partition. If the partition must be activated with the specified amount of processing resources, deactivate any active partitions using the resource then activate this partition.	<ol style="list-style-type: none"> 1. Ensure there is enough processing to start the partition. 2. Rebuild the managed system. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL03F6	The 5250 CPW needed by the partition exceeds the system limit. Amount allowable at this point is {0}.	<ol style="list-style-type: none"> 1. Check the 5250 CPW. 2. If the problem persists, contact your next level of support or your service provider.
HSCL03F7	Insufficient amount of 5250 CPW for allocation: Obtained - {0}, required - {1}.	<ol style="list-style-type: none"> 1. Ensure there are enough 5250 CPW to start the partition. 2. Rebuild managed system. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL03F8	The 5250 CPW set by user is below the partition minimum allowed: minimum = {0}.	<ol style="list-style-type: none"> 1. Ensure the 5250 CPW setting is correct. 2. If the problem persists, contact your next level of support or your service provider.
HSCL03F9	Not enough memory resources to meet the allocation setting.	<ol style="list-style-type: none"> 1. Ensure there is enough memory to start the partition. 2. Rebuild the managed system. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL03FA	Unable to gather I/O information of the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.

HSCL03xx error codes	Message	Recovery action
HSCL03FB	Unable to gather virtual I/O information of the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL03FC	The MAC address prefix specified was not valid. The MAC address prefix must be 6 characters long, and only contain hexadecimal values (0-9 and A-F).	<ol style="list-style-type: none"> 1. Ensure the MAC address conforms with the rule specified. 2. If the problem persists, contact your next level of support or your service provider.
HSCL03FD	The MAC address prefix cannot have the multicast bit on. The multicast bit is 0x010000.	<ol style="list-style-type: none"> 1. Ensure the multicast bit is not on 2. If the problem persists, contact your next level of support or your service provider.
HSCL03FE	There was an error updating a virtual Ethernet adapter MAC address.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL03FF	Failed to extract system resources information. Ensure the managed system is powered on.	<ol style="list-style-type: none"> 1. Retry the task. 2. Rebuild the managed system. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.

HSCL04xx logical partition error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCL04xx error codes	Message	Recovery action
HSCL0400	Failed to determine the minimum amount of memory required for the amount of maximum specified.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0401	Failed to determine the valid 5250 CPW range with the amount of processing given.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0402	Not enough system firmware memory is available to perform this task. The managed system needs an additional {0} MB of memory. You can free memory resources by removing memory through dynamic logical partitioning or by deleting partitions that are not being used.	The managed system needs additional memory. Remove memory through dynamic logical partitioning or deleting unused partitions to release memory resources.

HSCL04xx error codes	Message	Recovery action
HSCL0403	The number of processors available for i5/OS partitions is not sufficient: Obtained - {0}, Required - {1}. You can create a new profile or modify the existing profile to use the number of obtained processors, and then activate the partition. If the partition must be activated with the required number of processors, first shut down the active i5/OS partitions that are using the required processors, and then activate this partition.	<ol style="list-style-type: none"> 1. Create a new profile or modify the existing profile for the partition to use the number of obtained processors. 2. Alternatively, shut down other i5/OS partitions or use Dynamic Logical Partitioning to remove processing resources from other i5/OS partitions to release enough processors for this partition. Note: The number of i5/OS processors in use by an uncapped i5/OS partition is equivalent to the number of virtual processors in use by that partition. Therefore, in order to release i5/OS processors from an uncapped i5/OS partition, you must release virtual processors from that partition. Releasing one virtual processor from an uncapped i5/OS partition will release one physical i5/OS processor. 3. Try the task again.
HSCL0404	The number of shared processing resources available for i5/OS partitions is not sufficient: Obtained virtual processors - {0}, Required virtual processors - {1}, Obtained processing units - {2}, Required processing units - {3}. You can create a new profile or modify the existing profile to use the number of obtained processing resources, and then activate the partition. If the partition must be activated with the required number of processing resources, first shut down the active i5/OS partitions that are using the required processing resources, and then activate this partition.	<ol style="list-style-type: none"> 1. Create a new profile or modify the existing profile for the partition to use the number of obtained processing resources. 2. Alternatively, shut down other i5/OS partitions or use Dynamic Logical Partitioning to remove processing resources from other i5/OS partitions to release enough processing resources for this partition. Note: The number of i5/OS processors in use by an uncapped i5/OS partition is equivalent to the number of virtual processors in use by that partition. Therefore, in order to release i5/OS processors from an uncapped i5/OS partition, you must release virtual processors from that partition. Releasing one virtual processor from an uncapped i5/OS partition will release one physical i5/OS processor. Likewise, to assign one virtual processor to an uncapped i5/OS partition, one physical i5/OS processor must be available. 3. Try the task again.
HSCL0406	The maximum memory setting exceeds the maximum system memory capacity. Please check the capacity and modify the maximum memory setting in the profile accordingly.	Check the capacity and modify the maximum memory setting in the profile accordingly.
HSCL0407	Not enough huge page memory regions resources to meet the allocation setting.	<ol style="list-style-type: none"> 1. Ensure there is enough pages of huge page memory to start the partition. 2. Rebuild the managed system. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.

HSCL05xx logical partition error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

HSCL05xx error codes	Message	Recovery action
HSCL0500	<p>The operation violates the Workload Management Policy. It may be due to one of the following reasons:</p> <ol style="list-style-type: none"> 1. Deleting a partition which belongs to a cluster. 2. Changing a partition cluster ID from one cluster to another cluster. 3. Running dynamic partitioned move operation between two partitions which belong to the same cluster. 	<p>Check the operation.</p> <ol style="list-style-type: none"> 1. For deleting a clustered partition, first move it out of the cluster and then delete it. 2. For changing a cluster ID, first change it to a non-clustered partition, then change to the destination cluster. 3. It is not allowed to move processor or memory between two clusters.
HSCL0506	A Trial processor code to temporarily activate xx processors for yy days has been entered.	This is an informational message that is displayed after a Trial processor code has been entered using the Capacity On Demand Enter CoD Code task. This message is either followed by a message that indicates that the code was entered successfully, or it is followed by an error message if the code was rejected.
HSCL050F	The CoD code has been rejected by the managed system because it is not valid. Contact your CoD administrator.	This error message indicates that a CoD code that is entered is not valid for the managed system, even if it is a valid CoD code. This occurs when a CoD code is entered that was generated using information about the managed system that is incorrect, or a CoD code that was generated for a different managed system. Contact your CoD administrator to get a corrected CoD code.
HSCL0589	Could not delete partition {0}. Refresh the interface and check whether the operation was performed. If not, try the operation again.	<ol style="list-style-type: none"> 1. Refresh the interface and check whether the operation was performed. 2. If not, rebuild the managed system, and try the task again. For details, see Updating managed system or frame information. 3. If the operation still fails, contact your next level of support or your service provider.
HSCL058A	Could not activate the logical partition on logical partition {0} with ID {1}. Refresh the interface and check whether the operation was performed. If not, try the operation again.	<ol style="list-style-type: none"> 1. Perform a rebuild of the managed system. For details, see Updating managed system or frame information. 2. Try the task again. 3. If the operation still fails, contact your next level of support or your service provider.
HSCL058C	User defined name cannot be blank or empty.	<ol style="list-style-type: none"> 1. Set a non-blank user defined name for this partition. 2. If the problem persists, contact your next level of support or your service provider.
HSCL058D	The user defined name cannot be longer than {0} characters.	<ol style="list-style-type: none"> 1. The partition's user-defined name is too long. Shorten this partition's user-defined name, and try the operation again. 2. If the problem persists, contact your next level of support or your service provider.

HSCL05xx error codes	Message	Recovery action
HSCL058F	Cannot activate a LPAR when the managed system state is No Power.	<ol style="list-style-type: none"> 1. Verify that the managed system is in the Operating or Standby state and try the task again. 2. If the state is not Operating or Standby, refer to “Correcting the managed system operating state” on page 428 and perform the appropriate procedure to put the managed system in the correct state. 3. If the problem persists, contact your next level of support or your service provider.
HSCL059A	Cannot activate the logical partition. The profile’s maximum memory amount exceeds the managed system’s memory limit. Change the profile’s maximum memory amount.	Change the profile’s maximum memory amount, and retry the operation.
HSCL059D	This panel function is not enabled at this time.	
HSCL059E	Failed to get supported panel functions from firmware.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL05DB	The partition does not have Virtual IO Client capability.	
HSCL05DC	The partition does not have Virtual IO Server capability.	Choose the correct partition and retry the command.
HSCL05DD	Could not get logical partition state. Repeat the operation.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL05DE	A logical partition in the managed system already uses the name {0}. Provide another name for this logical partition.	Rename the logical partition to a name that is not yet used by other logical partitions in the same managed system. Refer to the logical partition help text for details.
HSCL05DF	The logical partition is not in a state under which this operation can be performed. Check the state of the logical partition.	<ol style="list-style-type: none"> 1. Verify that the operation is allowable under this logical partition state. 2. Refer to “Correcting the managed system operating state” on page 428 and perform the appropriate procedure to put the managed system in the correct state.
HSCL05E0	The logical partition {0} is in an undefined state. Rebuild the managed system.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Restart the HMC. 3. If the problem persists, contact your next level of support or your service provider.
HSCL05E1	Only {0} logical partitions can be allocated on this managed system can be allocated. There are no more unallocated logical partitions available. Delete unused or unwanted logical partitions for this managed system and retry the operation. Logical partitions in the ready state are currently not in use.	Delete unused or unwanted logical partitions. Logical partitions in the ready state are currently not in use. Refer to the logical partition help text for details.

HSCL05xx error codes	Message	Recovery action
HSCL05E2	Partition is in an unrecognized state.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Try the operation again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL05E3	Partition is in an unrecognized state.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Try the operation again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL05E5	Unable to create partition when the managed system is in {0} state. Ensure that the managed system is in the Operating or Standby state .	<ol style="list-style-type: none"> 1. Verify that the managed system is in the Operating or Standby state. 2. If it is not in the Operating or Standby state refer to “Correcting the managed system operating state” on page 428 and perform the appropriate procedure to put the managed system in the correct state. 3. If the problem persists, contact your next level of support or your service provider.
HSCL05E6	Logical partition {0} delete failed. Cannot delete a partition when its state is not in the Not Activated state. Perform a shut down operation then delete the partition.	<ol style="list-style-type: none"> 1. Verify the partition is in Not Activated state. 2. Perform a Rebuild Managed System operation. For details, see Updating managed system or frame information. 3. Then try the task again.
HSCL05E7	The profile you tried to activate does not belong to the logical partition {0} you specified. Select the correct LPAR profile.	Verify that you selected the correct logical partition profile to activate.
HSCL05E9	Could not activate the logical partition. Ensure that the partition is not already activated and that the managed system is in the Operating or Standby state.	<ol style="list-style-type: none"> 1. Verify that the logical partition is not already activated, and the state and power-on condition of the managed system are correct, and try the operation again. 2. If necessary, refer to “Correcting the managed system operating state” on page 428 and perform the appropriate procedure to put the managed system in the correct state. 3. If the problem persists, contact your next level of support or your service provider.
HSCL05EA	Cannot activate the partition when it is in state {0}. Ensure the partition is in the Not Activated state.	<ol style="list-style-type: none"> 1. Verify that the logical partition is not in the running, booting, or open firmware state. 2. If necessary, refer to “Correcting the managed system operating state” on page 428 and perform the appropriate procedure to put the managed system in the correct state. 3. If it still fails, contact your next level of support or your service provider.

HSCL05xx error codes	Message	Recovery action
HSCL05EB	Could not create the partition. Make sure that all requirements are met for creating a logical partition.	<ol style="list-style-type: none"> 1. To verify that all the requirements for creating a logical partition are met, refer to Partitioning the server. 2. If all requirements are met, do a rebuild of the managed system. For details, see Updating managed system or frame information. 3. Retry the task. 4. If the problem persists, contact your next level of support or your service provider.
HSCL05EC	Could not delete logical partition {0}. Ensure that all requirements are met for deleting a logical partition.	<ol style="list-style-type: none"> 1. Verify that all the requirements for deleting a logical partition are met. 2. Perform a rebuild of the managed system. For details, see Updating managed system or frame information. 3. Retry the task. 4. If it still fails, contact your next level of support or your service provider.
HSCL05ED	Could not set the properties for logical partition {0}. Try again	<ol style="list-style-type: none"> 1. Repeat the operation. 2. If the operation still fails, contact your next level of support or your service provider.
HSCL05EE	Could not get the managed system's service provider. processor log entry. Try again	<ol style="list-style-type: none"> 1. Repeat the operation. 2. If the operation still fails, contact your next level of support or your service provider.
HSCL05EF	This new logical partition does not have a user-defined name. Specify a name for the logical partition.	<ol style="list-style-type: none"> 1. Set the user-defined name for this logical partition. For details, see Viewing information about the managed system. 2. If it still fails, contact your next level of support or your service provider.
HSCL05F3	Could not display the OS reset dialog for logical partition {0}. Try again.	<ol style="list-style-type: none"> 1. Refresh the interface and check whether the operation was performed. 2. If not, rebuild the managed system. For details, see Updating managed system or frame information. 3. Retry the task. 4. If the operation still fails, contact your next level of support or your service provider.
HSCL05F4	Could not display the logical partition activate dialog for logical partition {0}. Try again.	<ol style="list-style-type: none"> 1. Log off and then log in to the HMC and try the operation again. 2. If this does not correct the problem, contact your next level of support or your service provider.
HSCL05F5	Could not display the create logical partition dialog for the managed system: {0}. Try again.	<ol style="list-style-type: none"> 1. Log off and then log in to the HMC and try the operation again. 2. If this does not correct the problem, contact your next level of support or your service provider.

HSCL05xx error codes	Message	Recovery action
HSCL05F7	Could not open the virtual terminal for logical partition {0} with ID {1}.	<ol style="list-style-type: none"> 1. Refresh the interface and check whether the operation was performed. 2. If not, rebuild the managed system, and try the task again. For details, see Updating managed system or frame information. 3. If the operation still fails, contact your next level of support or your service provider.
HSCL05F8	Could not perform the OS reset {0} reset on logical partition {1} with ID {2}.	<ol style="list-style-type: none"> 1. Refresh the interface and check whether the operation was performed. 2. If not, rebuild the managed system, and try the task again. For details, see Updating managed system or frame information. 3. If the operation still fails, contact your next level of support or your service provider.
HSCL05F9	Could not delete logical partition {0}. Refresh the interface and check whether the operation was performed. If not, try the operation again.	<ol style="list-style-type: none"> 1. Verify that the logical partition displays on the graphical user interface. 2. Delete the logical partition again, and check the graphical user interface to see if it is updated appropriately. 3. Log off and log back in to the HMC. 4. Contact your next level of support or your service provider.

HSCL06xx error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

Back to HSCL error codes page

HSCL06xx error codes	Message	Recovery action
HSCL0601	Cannot create partition with bootable definition state setting.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0602	Partition with the same ID is already defined in the managed system.	<ol style="list-style-type: none"> 1. Check the entry and try again. 2. Rebuild the managed system. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0604	Could not read the dump.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0605	The initialize dump request failed because the managed system is already in the process of creating a dump of the specified type.	The keylock position of the managed system needs to be set to manual mode.

HSCL06xx error codes	Message	Recovery action
HSCL0607	Dump partition does not exist.	<ol style="list-style-type: none"> 1. Ensure that the dump partition has been mounted. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0608	Could not mount the dump partition.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0611	Could not read dump as a temporary file.	<ol style="list-style-type: none"> 1. Ensure that the dump partition has been mounted and has an access to it. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0612	Could not process dump header.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0613	Could not query the dump.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0616	Cannot use the 5250 CPW setting. Check whether the setting is valid.	<ol style="list-style-type: none"> 1. Ensure the 5250 CPW setting is correct. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0619	Cannot use the I/O setting for allocation. Check whether the setting is valid.	<ol style="list-style-type: none"> 1. Check the I/O setting is valid. 2. Rebuild the managed system. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL061A	Cannot use the virtual I/O setting for allocation. Check whether the setting is valid.	<ol style="list-style-type: none"> 1. Check that the setting is valid 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL061B	Operation failed to set partition activation policies.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL061C	Operation failed to allocate memory for the partition.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL061D	Operation failed to allocate virtual I/O for the partition.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.

HSCL06xx error codes	Message	Recovery action
HSCL061E	Operation failed to allocate 5250 CPW for the partition.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL061F	Operation failed to allocate processing resource for the partition.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0620	Operation failed to allocate I/O slots for the partition.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0621	Cannot use the LPAR profile for partition operation since its dedicated processor setting is not correct. Check the processor setting in the profile, and ensure the setting is valid.	<ol style="list-style-type: none"> 1. Check the processors settings 2. If the problem persists, contact your next level of support or your service provider.
HSCL0622	Cannot use the LPAR profile for partition operation since its shared processor setting is not correct. Check the processor setting in the profile, and ensure the setting is valid.	<ol style="list-style-type: none"> 1. Check the processors settings 2. If the problem persists, contact your next level of support or your service provider.
HSCL0623	Partition cluster ID cannot be modified when the partition is not in the Not Activated state.	<ol style="list-style-type: none"> 1. Ensure the partition is in <i>Not Activated state</i>. 2. Rebuild the managed system. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0624	Unable to launch Update Password Dialog. Try again.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0625	Cannot activate partition when the managed system state is not in the Operating or Standby state.	<ol style="list-style-type: none"> 1. Ensure the partition is in Operating or Standby state. 2. Rebuild the managed system. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0626	Cannot find the LPAR profile to activate the partition.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.

HSCL06xx error codes	Message	Recovery action
HSCL0627	The virtual I/O specified for tagged I/O is not valid.	<ol style="list-style-type: none"> 1. Check that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0628	Resource specified as load source must be required.	<ol style="list-style-type: none"> 1. Ensure the load source device is specified as required. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0629	Must specify resource for load source setting.	<ol style="list-style-type: none"> 1. Ensure the load source device is specified as required. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL062A	Cluster ID specified, {0}, is greater than maximum allowable value, {1}.	<ol style="list-style-type: none"> 1. Ensure the setting is valid. 2. Retry the operation.
HSCL062B	Cannot change maximum virtual I/O Slots value when partition is not in the Not Activated state.	<ol style="list-style-type: none"> 1. Ensure the setting is valid. 2. Retry the operation.
HSCL062D	The partition is currently in a state of Running, Initializing or Open Firmware, and cannot be deleted.	<p>A partition cannot be deleted when it is in Running, Initializing, or Open Firmware state.</p> <ol style="list-style-type: none"> 1. Deactivate the partition and retry the operation. 2. If you believe that the partition is already stopped, rebuild the managed system. For details, see Updating managed system or frame information. 3. Retry the operation. 4. If the problem persists, contact your next level of support or your service provider.
HSCL062E	Unable to shut down the partition using operation system command.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL062F	You must select one profile to activate the partition with or select Cancel.	<ol style="list-style-type: none"> 1. Only one partition profile can be used to activate a partition. Either retry the operation, selecting a profile to activate the partition with, or select Cancel. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0630	Could not display the partition activate advance dialog for partition: {0}. Try the operation again.	<ol style="list-style-type: none"> 1. Refresh the graphical user interface and retry the operation. For details, see Updating managed system or frame information. 2. Log off and then log back in to the HMC and try the operation again. 3. If the problem persists, contact your next level of support or your service provider.

HSCL06xx error codes	Message	Recovery action
HSCL0631	Could not display the partition reboot dialog. Try the operation again.	<ol style="list-style-type: none"> 1. Refresh the graphical user interface and retry the operation. For details, see Updating managed system or frame information. 2. Log off and then log back in to the HMC and try the operation again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0632	Could not perform the reboot partition operations. Refresh the interface and check whether the operation was performed. If not, try the operation again.	<ol style="list-style-type: none"> 1. Refresh the interface and check whether the operation was performed. 2. If not, rebuild the managed system. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0633	Could not display the partition shut down dialog. Try the operation again.	<ol style="list-style-type: none"> 1. Refresh the graphical user interface and retry the operation. For details, see Updating managed system or frame information. 2. Log off and then log back in to the HMC and try the operation again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0634	Could not perform the shut down partition operations. Refresh the interface and check whether the operation was performed. If not, try the operation again.	<ol style="list-style-type: none"> 1. Refresh the interface and check whether the operation was performed. 2. If not, rebuild the managed system. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0635	Could not display the change default profile dialog. Try the operation again.	<ol style="list-style-type: none"> 1. Refresh the graphical user interface and retry the operation. For details, see Updating managed system or frame information. 2. Log off and then log back in to the HMC and try the operation again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0636	Unable to modify processing information of the partition with ID of {0}. The information could be out of sync. Rebuild the managed system and try again.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0637	Unable to modify processing information of the partition with ID of {0}. The information could be out of sync. Rebuild the managed system and try again.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0638	Unable to modify 5250 CPW information of the partition with ID of {0}. Rebuild the managed system and try again.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.

HSCL06xx error codes	Message	Recovery action
HSCL0639	Unable to modify OptiConnect setting of the partition with ID of {0}. Rebuild the managed system and try again.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL063A	Unable to extract partition's virtual I/O information.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL063B	Failed to set I/O adapter {0} for the partition.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL063C	Failed to set tagged I/Os for the partition.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL063D	Failed to change the partition's processor type.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL063E	Failed to change the partition's processor settings.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL063F	Cannot assign a storage device under I/O processor to AIX/Linux partition.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0640	OptiConnect Pool IDs may only be set on i5/OS partitions.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0641	Cannot activate a profile using full system resources while other partitions are powered on.	<ol style="list-style-type: none"> 1. Ensure there are no partitions running. 2. Rebuild the managed system. For details, see Updating managed system or frame information. 3. Retry the task. 4. If the problem persists, contact your next level of support or your service provider.

HSCL06xx error codes	Message	Recovery action
HSCL0642	Partition ID specified is over max number of partition supported by the system. Check the entry and try again.	<ol style="list-style-type: none"> 1. Ensure the partition ID specified does not exceed the maximum number of logical partitions supported. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0643	Virtual I/O server command {0} for partition {1} failed.	The I/O server command for the partition failed. The reason or cause is included in the error message. Check the command and retry. If the error persists, contact your next level of support or your service provider.
HSCL0644	The number of processing units must be less than or equal to the number of virtual processors.	In the partition profile properties, make sure the number of processing units is less than or equal to the number of virtual processors.
HSCL0645	The ratio of processing units to virtual processors must be equal to or greater than {0}.	In the partition profile properties, make sure the ratio of processing units to virtual processors is equal to or greater than the value that is specified.
HSCL0646	Processor pool ID specified is over maximum processor pools system allowed.	Make sure the processor pool ID specified is not over the maximum processor pools system allowed.
HSCL0647	The workload group setting for the partition could not be changed. Try the operation again. If the problem persists, contact your technical support provider.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0648	The setting for power controlling partitions could not be changed. Try the operation again. If the problem persists, contact your technical support provider.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0649	The opticonnect settings for the partition could not be changed. Try the operation again. If the problem persists, contact your technical support provider.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL064A	Cannot use the SMA setting for allocation. Check whether the setting is valid.	
HSCL064B	Cannot use the HCA setting for allocation. Check whether the setting is valid.	Ensure that this HCA adapter is not allocated to another Active partition and retry the operation.
HSCL0650	An i5/OS partition or profile is not allowed to use all the resources in a IBM System p5 or IBM eServer p5 server.	
HSCL0651	The maximum number of processors specified exceeds the i5/OS processor capacity limit of {0} processors for the managed system. Reduce the number and try again.	<ol style="list-style-type: none"> 1. Reduce the number specified for the maximum number of processors to a number that is less than or equal to the i5/OS processor capacity limit for your managed system. 2. Try the task again.

HSCL06xx error codes	Message	Recovery action
HSCL0652	The maximum number of processing units specified exceeds the i5/OS processor capacity limit of {0} processing units for the managed system. Reduce the number and try again.	<ol style="list-style-type: none"> 1. Reduce the number specified for the maximum number of virtual processors to a number that is less than or equal to the i5/OS processor capacity limit for your managed system. 2. Try the task again.
HSCL0653	The maximum number of virtual processors specified exceeds the i5/OS processor capacity limit of {0} processors for the managed system. Reduce the number and try again.	<ol style="list-style-type: none"> 1. Reduce the number specified for the maximum number of processing units to a number that is less than or equal to the i5/OS processor capacity limit for your managed system. 2. Try the task again.
HSCL0654	The HCA device {0} has a hardware error. You cannot active the profile containing a GUID from this device. Clear the adapter configuration from the profile and try again or contact your service provider.	If the device is needed for the partition, contact your next level of support or service provider.
HSCL0655	The profile contains a GUID for an HCA device {0} not managed by the HMC. Clear the adapter configuration from the profile and try again.	If the device should be managed from the HMC, or if the device is needed for the partition, contact your next level of support or service provider.

HSCL07xx error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCL07xx error codes	Message	Recovery action
HSCL07C0	The virtual SCSI server adapter cannot be created because the partition does not have virtual I/O server capability. Only i5/OS partitions in IBM System i5, eServer i5, or virtual I/O server partitions have virtual I/O server capability.	
HSCL07C1	The virtual serial client adapter cannot be created because the partition does not have virtual I/O server capability.	
HSCL07C2	Managed system was in checkstop state and unable to send the dump. A post-checkstop IPL was initiated. Please retry the operation.	<ol style="list-style-type: none"> 1. Perform the operation again after the system was re-IPLed. 2. If the problem persists, contact your next level of support or your service provider.
HSCL07C5	This operation cannot be performed because the HMC is not connected to service processor. Check the connection and try the operation again	<ol style="list-style-type: none"> 1. Ensure that the HMC is connected to the service processor. 2. If the problem persists, contact your next level of support or your service provider.

HSCL07xx error codes	Message	Recovery action
HSCL07C6	Cannot use the huge page memory regions resource setting. Check whether the setting is valid or not.	<ol style="list-style-type: none"> 1. Ensure the page setting is correct. 2. If the problem persists, contact your next level of support or your service provider.
HSCL07C7	There is not enough huge page memory regions: Obtained : {0}, Required : {1}. Check that there is enough huge page memory regions available to activate the partition. If not, create a new profile or modify the existing profile with the available resources, then activate the partition. If the partition must be activated with these resources, deactivate any running partition(s) using the resource then activate this partition.	<ol style="list-style-type: none"> 1. Check the managed system properties window to ensure that enough pages of huge page memory is available to activate the partition. 2. If there is not enough available pages of huge page memory, create a new profile or modify the existing profile with the available resources and then activate the partition. 3. If the partition must be activated at any cost, deactivate any running partition using the resource, and activate the partition. 4. If the problem persists, contact your next level of support or your service provider.
HSCL07C8	Operation failed to allocate huge page memory regions for the partition."	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL07D0	This partition is not bootable therefore a profile cannot be generated according to the partition's current configuration.	A "Save profile" cannot be done when the partition is not bootable. The resource of this partition might have been taken by another partition. Try to activate the partition with an appropriate profile.
HSCL07D1	This logical partition profile is currently active in its logical partition and cannot be modified or deleted. To make the profile inactive, bring the partition to the Not Activated state, then repeat the operation.	<p>Partition profiles that are active in a logical partition cannot be deleted.</p> <ol style="list-style-type: none"> 1. Perform an operating system reset on the partition to bring it to the Not Activated state, at which time the profile will no longer be active. For details, see Resetting the operating system on a partition . 2. If it still fails, contact your next level of support or your service provider.
HSCL07D2	This logical partition profile is the logical partition's default profile and cannot be deleted. If you still want to delete it, change the default profile for this logical partition or, if necessary, create another logical partition profile to be the default profile.	<p>All logical partitions must have at least one partition profile, which is designated as the default profile because it is the profile implicitly used when the logical partition is activated with no profile specified.</p> <ol style="list-style-type: none"> 1. If you still want to delete it, change the default profile for this logical partition (create another logical partition profile if necessary). 2. If it still fails, contact your next level of support or your service provider.
HSCL07D3	The logical partition profile could not be found in the HMC save area. The HMC is either out of sync with the console save area, or the console save area has been corrupted. Rebuild this logical partition profile's managed system.	<ol style="list-style-type: none"> 1. Ensure that the inputs are correct. 2. Restore the profile data. For details, see Restoring profile data. 3. If the problem persists, contact your next level of support or your service provider.

HSCL07xx error codes	Message	Recovery action
HSCL07D4	A profile named {0} already exists for this logical partition in the Hardware Management Console save area. Choose a different name for the new system profile.	<ol style="list-style-type: none"> 1. All partition profiles for a logical partition must have unique names. Choose a different name for the new profile. 2. If the problem persists, contact your next level of support or your service provider.
HSCL07D8	Deleting default profile associations within the current context is not allowed.	
HSCL07D9	Setting a default profile association is only allowed during create.	
HSCL07DA	The logical partition profile used for the operation cannot be found in the profile data.	<ol style="list-style-type: none"> 1. Verify that you entered the correct information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL07DB	An attempt to create a profile failed.	<ol style="list-style-type: none"> 1. Try the task again. 2. If problem persists, contact your next level of support or your service provider.
HSCL07DC	An attempt to modify a profile failed.	<ol style="list-style-type: none"> 1. Try the task again. 2. If problem persists, contact your next level of support or your service provider.
HSCL07DD	The LPAR profile's processing resources setting is not valid. Check profile processing resource setting.	<ol style="list-style-type: none"> 1. Check the processing resources setting. 2. If the problem persists, contact your next level of support or your service provider.
HSCL07DE	The LPAR profile's 5250 CPW setting is not valid. Check profile processing resource setting.	<ol style="list-style-type: none"> 1. Check the 5250 CPW. 2. If the problem persists, contact your next level of support or your service provider.
HSCL07DF	Virtual slot 0 and 1 are set to default as virtual serial adapters when a partition is created. No modification can be made regarding these 2 slots.	
HSCL07E0	The partition profile could not be found in the database. Perform a rebuild managed system operation, and try again.	<ol style="list-style-type: none"> 1. Rebuild the managed system. See Updating managed system or frame information for details. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL07E1	An error occurred while changing the default profile for the partition. Retry the operation.	<ol style="list-style-type: none"> 1. Rebuild the managed system. See Updating managed system or frame information for details. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL07E2	Required processor information is not specified in the partition profile. Make sure values are provided in the partition profile for minimum processing units, desired processing units, maximum processing units, processing mode, and sharing mode.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Try the task again. 3. If the problem persists, contact your next level of support or your service provider.

HSCL07xx error codes	Message	Recovery action
HSCL07E3	Failed to delete LPAR profile, {0}, from partition, {1}.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service.
HSCL07E5	The critical I/O setting is incorrect. Check the setting and try again.	<ol style="list-style-type: none"> 1. Ensure the tagged I/O setting is correct. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL07E8	SNI device IDs may not be specified in this profile because the managed system does not support SNI message passing.	No recovery action is needed.
HSCL07E9	SNI device IDs may not be specified in this profile because the partition is not AIX or Linux.	No recovery action is needed.
HSCL07EA	SNI device IDs may not be specified in this profile because no SNI adapters are installed in the managed system.	

HSCL09xx system profile error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCL09xx error codes	Message	Recovery action
HSCL09C6	Could not find the system profile in memory. It might be corrupted. Restore the profile data.	<p>The system profile might be corrupted.</p> <ol style="list-style-type: none"> 1. Restore the profile data. For details, see Restoring profile data. 2. If the problem persists, delete and re-create a new system profile. Refer to Creating a system profile. 3. If the problem persists, contact your next level of support or your service provider.
HSCL09C7	A system profile named {0} already exists for this managed system in the Hardware Management Console save area. Choose a different name for the new system profile.	Every system profile created for an individual managed system must have a unique name. Choose a different name for the new system profile. If it still fails, contact your next level of support or your service provider.
HSCL09C8	Could not open the Copy System Profile dialog. Try again.	<ol style="list-style-type: none"> 1. Log off the HMC, and log back in. 2. Try the task again. For details, see Copy a system profile. 3. If it still fails, contact your next level of support or your service provider.
HSCL09C9	Could not copy the system profile {0}. Try again.	<ol style="list-style-type: none"> 1. Log off the HMC, and log back in. 2. Try the task again. Refer to Copy a system profile. 3. If it still fails, contact your next level of support or your service provider.

HSCL09xx error codes	Message	Recovery action
HSCL09CA	Could not delete the system profile. Try the task again.	<ol style="list-style-type: none"> 1. Log off the HMC, and log back on. 2. Try the task again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL09CF	Validation of system profile failed. Retry the operation.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL09D0	Cannot validate system profile if the managed system is not in Operating or Standby state.	<ol style="list-style-type: none"> 1. Ensure that the managed system is in the Operating or Standby state and then retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL09D2	The following partition or partitions failed to activate: {0}	<p>A logical partition that is part of the system profile failed to activate.</p> <ol style="list-style-type: none"> 1. Ensure that you have enough available resources to activate the desired partition profile. 2. If so, rebuild the managed system. For details, see Updating managed system or frame information. 3. Retry the operation. 4. If the problem persists, contact your next level of support or your service provider.
HSCL09D3	An unknown error occurred during system profile activation. Retry the operation.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL09D4	Update of the system profile failed. Retry the operation.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL09D5	An unknown error occurred during system profile creation. Retry the operation.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL09D6	An unknown error occurred during deletion of the system profile. Retry the operation.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.

HSCL09xx error codes	Message	Recovery action
HSCL09D7	The system profile that you have chosen to validate could not be found.	<p>The system profile might be corrupted.</p> <ol style="list-style-type: none"> 1. Restore the profile data. For details, see Restoring profile data. 2. If the problem persists, delete and re-create a new system profile. 3. If the problem persists, contact your next level of support or your service provider.
HSCL09D8	System profile {0} could not be {1} because profile {2} was not found in the managed system.	<p>A profile that is part of the system profile cannot be found in the managed system.</p> <ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL09D9	System profile {0} could not be {1} because profiles {2} and {3} belong to the same partition. Take one of the profiles out of the system profile list and try again.	<p>There is more than one profile in the system profile that belongs to the same partition.</p> <ol style="list-style-type: none"> 1. Ensure that each partition has at most one profile in the system profile, and retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL09DA	System profile {0} could not be {1} because LPAR profile {2}, belonging to partition {3}, is listed more than once. Take one of the profiles out of the system profile list and try again.	<p>A profile is listed more than once in the system profile.</p> <ol style="list-style-type: none"> 1. Ensure that all partition profiles are only listed once in the system profile, and retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL09DB	Partition {0} could not be activated because it is already active.	<p>This error occurs when a logical partition listed in the system profile is already activated.</p> <ol style="list-style-type: none"> 1. If the logical partition is not activated, rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL09DC	System profile {0} could not be {1} because profile {2} is a full system partition profile. There cannot be any other partition profiles listed in the system profile.	<p>If a full system partition profile is part of a system profile, there can be no other partition profiles listed in that system profile.</p> <ol style="list-style-type: none"> 1. Either take all other profiles except the full system partition profile out of the system profile, or remove the full system partition profile from the system profile. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL09DD	The partition profile ID {0} does not correspond to a valid profile. Retry the command.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.

HSCL09xx error codes	Message	Recovery action
HSCL09DE	The system profile cannot be created because no user-defined name was given. Ensure to enter a user-defined name, and try the operation again.	<ol style="list-style-type: none"> 1. No user-defined system profile name was given during system profile creation. Retry the creation operation again, this time making sure to enter a user-defined name. 2. If the problem persists, contact your next level of support or your service provider.
HSCL09DF	The system profile cannot be created because there are no partition profiles currently included in the system profile. Specify partition profiles for the system profile or click \"Cancel\" .	<ol style="list-style-type: none"> 1. Partition profiles for the system profile must be specified during system profile creation. Retry the system profile creation operation, making sure to add at least one partition profile to the system profile. 2. If the problem persists, contact your next level of support or your service provider.
HSCL09E0	The profile {0} belongs to a partition that currently has a profile already included in the system profile. Select a profile from a different partition or first remove the conflicting partition's profile from the system profile, then add the desired profile again.	
HSCL09E1	There is currently a system profile with the name {0} created for this system. Enter a unique name.	<ol style="list-style-type: none"> 1. If there is not a system profile with the specified name displayed in the console, refresh the console and try the command again. 2. If it fails again, rebuild the managed system. For details, see Updating managed system or frame information. 3. Restart the HMC and then try the task again. 4. If the problem persists, contact your next level of support or your service provider.
HSCL09E2	Validation results for system profile {0}:{1}.	This message is for informational purposes only regarding the outcome of system profile validation. No recovery action should be taken.
HSCL09E3	Activation results for system profile {0}:{1}.	This message is for informational purposes only regarding the outcome of system profile validation. No recovery action should be taken.

HSCL0Bxx attention light messages

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCL0Bxx error codes	Message	Recovery action
HSCL0BBB	Can not get LED.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the operation. 3. Restart the HMC and then try the task again. 4. If the problem persists, contact your next level of support or your service provider.

HSCL0Dxx operating system reset error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCL0Dxx error codes	Message	Recovery action
HSCL0DB2	An operating system reset can be issued for a logical partition only if the partition is in the running or starting state.	<ol style="list-style-type: none">1. Rebuild the managed system. For details see Updating managed system or frame information.2. Try the task again.
HSCL0DB4	An Operating System shut down can not be performed because the operating system image running does not support remote execution of this task from the HMC.	<ol style="list-style-type: none">1. Ensure the network connection between partition and HMC is working.2. Rebuild the HMC. For details see Updating managed system or frame information.3. If the problem persists, contact your next level of support or your service provider.
HSCL0DB5	An Operating System Shut down can be issued for a logical partition only if the partition is in the Running state.	<p>A partition must be in the Running state in order for an operating system shutdown operation to be performed.</p> <ol style="list-style-type: none">1. Ensure that the partition's state is Running, and try the task again.2. If your partition is in a state other than Running, but you are sure that the partition is in fact running, rebuild the managed system. For details, see Updating managed system or frame information.3. Retry the operation.4. If the problem persists, contact your next level of support or your service provider.
HSCL0DB7	Fail to shut down partition through operation system command due to following reasons: {0}.	<ol style="list-style-type: none">1. Ensure that the network between the HMC and the partition is working.2. Retry the operation.3. If the problem persists, contact your next level of support or your service provider.

HSCL0Fxx error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCL0Fxx error codes	Message	Recovery action
HSCL0FA6	Connection has closed.	Connection was closed by you or another user. Close the window and open another terminal session.

HSCL0Fxx error codes	Message	Recovery action
HSCL0FA7	<p>The open failed.</p> <p>1) The session may already be open on another management console</p> <p>2) The server may not be ready to accept connections.</p>	<ol style="list-style-type: none"> 1. Try the “Close Terminal Connection” task then retry to open the session again. Note: Closing the session will terminate the session of other users. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0FA8	Error in communication path to the partition.	<p>The managed system is not accepting connections.</p> <ol style="list-style-type: none"> 1. Check the network connection to the server. 2. Wait for few minutes and retry the connection. 3. If the connection still fails, restart the HMC. 4. If the problem persists, contact your next level of support or your service provider.
HSCL0FA9	Internal error encountered	<ol style="list-style-type: none"> 1. Wait for few minutes and retry the connection. 2. Shut down and restart the HMC. 3. If the problem persists, contact your next level of support or your service provider.
HSCL0FAA	<p>Lost connection to the Managed System.</p> <p>Attempting to reconnect</p>	A network problem has been encountered, or the service processor has gone offline. The session is attempting to reconnect to the server. If the server state is in ‘No Connection’ or ‘Error’ state, then the connection attempt will fail.
HSCL0FAB	<p>A terminal session is already open for this partition.</p> <p>Only one open session is allowed for a partition.</p>	<p>Another user is using the virtual terminal for this partition. Use the “Close Terminal Connection” task to disconnect the other session.</p> <p>Note: Closing the session will terminate the session of the other user.</p>
HSCL0FAC	<p>A terminal session is already open for this partition.</p> <p>Only one open session is allowed for a partition.</p> <p>Exiting</p>	<p>Another user is using the virtual terminal for this partition. Use the “Close Terminal Connection” task to disconnect the other session.</p> <p>Note: Closing the session will terminate the session of the other user.</p>
HSCL0FAD	<p>The connection to the server is not available.</p> <p>Exiting.</p>	<p>A network problem has been encountered, or the service processor has gone offline.</p> <ol style="list-style-type: none"> 1. Wait for few minutes and retry the connection. 2. Ensure the network connection between the HMC and the managed system is good. 3. Shut down and restart the HMC. 4. If the problem persists, contact your next level of support or your service provider.
HSCL0FAE	The connection to the server is not available.	<p>A network problem has been encountered, or the service processor has gone offline.</p> <ol style="list-style-type: none"> 1. Wait for few minutes and retry the connection. 2. Ensure the network connection between the HMC and the managed system is good. 3. Shut down and restart the HMC. 4. If the problem persists, contact your next level of support or your service provider.

HSCL0Fxx error codes	Message	Recovery action
HSCL0FAF	Received invalid connection information. Operation cancelled.	<ol style="list-style-type: none"> 1. Close the terminal window and open another window. 2. If the problem persists, contact your next level of support or your service provider.
HSCL0FB0	Received invalid connection information. Operation cancelled. Exiting.	<ol style="list-style-type: none"> 1. Close the terminal window and open another window. 2. If the problem persists, contact your next level of support or your service provider.

HSCL11xx backup and restore error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCL11xx error codes	Message	Recovery action
HSCL1195	Unable to back up the profile data to the backup file. Try again.	<ol style="list-style-type: none"> 1. Try the task again. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1196	You do not have read access permission on the backup file {0}. Refresh the interface and check whether the operation was completed. If not, try the operation again.	<ol style="list-style-type: none"> 1. Try the task again. 2. If the operation still fails, contact your next level of support or your service provider.
HSCL1197	Unable to read the profile data's backup file {0}. Refresh the interface and check whether the operation was completed. If not, try the operation again.	<ol style="list-style-type: none"> 1. Try the task again. 2. Shut down and restart the HMC, and then try the task again. 3. If the operation still fails, contact your next level of support or your service provider.
HSCL1198	Cannot find backup file {0} for profile data. Select a valid, existing backup file.	<ol style="list-style-type: none"> 1. Try the task again. 2. If the operation still fails, contact your next level of support or your service provider.
HSCL1199	A full restore is not permitted when there are logical partitions in {0} state. A full restore can only be issued when the managed system was powered on and all partitions are in the Not Activated state.	<ol style="list-style-type: none"> 1. Verify the managed system was powered-on to run in Partition Standby. 2. Try the task again. 3. If the operation still fails, contact your next level of support or your service provider.
HSCL119A	There was an I/O error while backing up the profile data. Try again.	<ol style="list-style-type: none"> 1. Try the task again. 2. Shut down and restart the HMC, and then try the task again. 3. If the operation still fails, contact your next level of support or your service provider.

HSCL11xx error codes	Message	Recovery action
HSCL119B	The restore profile data operation failed. Try again.	<ol style="list-style-type: none"> 1. Try the task again. 2. Shut down and restart the HMC, and then try the task again. 3. If the operation still fails, contact your next level of support or your service provider.
HSCL119C	Cannot initialize profile data when the managed system was not in the Standby or Operating state, or there is any partition not in the Not Activated state.	<ol style="list-style-type: none"> 1. Verify that the managed system is in the Standby or Operating state, and that no logical partitions are running. 2. Try the task again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL119D	Cannot restore the profile data if the managed system is in the {0} state.	<ol style="list-style-type: none"> 1. Verify that the managed system is in the Standby or Ready state, and try the task again. 2. If the problem persists, contact your next level of support or your service provider.
HSCL119E	Cannot initialize the profile data if the managed system is in the {0} state.	<ol style="list-style-type: none"> 1. Verify that the managed system is in the Standby or Ready state, and try the task again. 2. If the problem persists, contact your next level of support or your service provider.
HSCL119F	The backup file {0} used to restore the profile data is not valid. Its file size {1} is not correct. Select a valid backup file.	<p>The backup file selected is not valid. The file might be corrupted.</p> <ol style="list-style-type: none"> 1. Try the task again. 2. Select another backup file and try the task again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL11A0	Cannot restore the profile data if the managed system is in the {0} state. The managed system must be in the Operating or Standby state.	<ol style="list-style-type: none"> 1. Verify that the managed system is in Operating or Standby state. 2. Try the task again.
HSCL11A1	Cannot initialize the profile data if the managed system is in the {0} state. The managed system must be in the Operating or Standby state.	<ol style="list-style-type: none"> 1. Verify that the managed system is in Operating or Standby state. 2. Try the task again.
HSCL11A2	Could not display the backup dialog for the managed system: {0}. Try the operation again.	<ol style="list-style-type: none"> 1. Try the task again. 2. Log off the HMC, and then log back in. 3. Try the task again. 4. If the problem persists, contact your next level of support or your service provider.
HSCL11A3	Could not back up the profile data for the managed system: {0} to file {1}.	<ol style="list-style-type: none"> 1. Refresh the graphical user interface. For details, see Updating managed system or frame information. 2. Try the task again. 3. Shut down and restart the HMC, and then try the task again. 4. If the problem persists, contact your next level of support or your service provider.

HSCL11xx error codes	Message	Recovery action
HSCL11A4	Cannot back up profile data to the default backup file name {0}.	Cannot back up the profile data to the default backup file. Choose a different backup file name. If the problem persists, contact your next level of support or your service provider.
HSCL11A5	Could not display the remove backup dialog for the managed system {0}. Try again.	<ol style="list-style-type: none"> 1. Try the task again. 2. Log off the HMC, and log back in. 3. Try the task again. 4. contact your next level of support or your service provider.
HSCL11A6	Could not remove the backup file {0} from the managed system {1}.	<ol style="list-style-type: none"> 1. Refresh the graphical user interface. For details, see Updating managed system or frame information. 2. Try the task again. 3. Shut down and restart the HMC, and then try the task again. 4. If the problem persists, contact your next level of support or your service provider.
HSCL11A7	No backup file has been selected for the operation. Select a backup file.	If the problem persists, contact your next level of support or your service provider.
HSCL11A8	Could not display the restore profile data dialog for the managed system: {0}. Try the operation again.	<ol style="list-style-type: none"> 1. Try the task again. 2. Log off the HMC, and then log back in. 3. Try the task again. 4. If the problem persists, contact your next level of support or your service provider.
HSCL11A9	Could not initialize the profile data task on the managed system {0}. Refresh the interface and check whether the operation was performed. If not, try the operation again.	<ol style="list-style-type: none"> 1. Refresh the graphical user interface. For details, see Updating managed system or frame information. 2. Ensure the operation has been performed and displays on the graphical user interface. 3. If not, repeat the operation. 4. If the problem persists, contact your next level of support or your service provider.
HSCL11AA	Could not restore the profile data task on the managed system {0} with backup file {1} of {2} option. Refresh the interface and check whether the operation was performed. If not, try the operation again.	<ol style="list-style-type: none"> 1. Refresh the graphical user interface. For details, see Updating managed system or frame information. 2. Try the task again. 3. Rebuild the managed system. For details, see Updating managed system or frame information. Then try the task again. 4. If the problem persists, contact your next level of support or your service provider.
HSCL11AB	Could not display the recover partition data dialog for the managed system {0}.	<ol style="list-style-type: none"> 1. Try the task again. 2. Log off the HMC, and then log back in. 3. Try the task again. 4. If the problem persists, contact your next level of support or your service provider.

HSCL11xx error codes	Message	Recovery action
HSCL11AC	Could not perform the recover logical partition data task on the managed system {0}.	<ol style="list-style-type: none"> 1. Refresh the graphical user interface. For details, see Updating managed system or frame information. 2. Try the task again. 3. Rebuild the managed system. For details, see Updating managed system or frame information. 4. If the problem persists, contact your next level of support or your service provider.
HSCL11AD	Could not display the Rebuild Computer System dialog for managed system {0}.	<ol style="list-style-type: none"> 1. Refresh the graphical user interface and retry the operation. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.

HSCL13xx utility class error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCL13xx error codes	Message	Recovery action
HSCL138F	Could not get the Hardware Management Console host name. Check the network settings within the system configuration.	<ol style="list-style-type: none"> 1. Check the network setting under system configuration, and then try the task again. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1393	Could not load the list of IBM PC product names.	<ol style="list-style-type: none"> 1. Shut down and restart the HMC. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1395	Could not launch the Confirmation dialog. Try again.	<ol style="list-style-type: none"> 1. Refresh the graphical user interface. See Updating managed system or frame information for details. 2. Try the task again. 3. Log off and then log back in to the HMC and try the operation again. 4. If the problem persists, contact your next level of support or your service provider.
HSCL1397	Could not determine the version of the firmware that is loaded on the service processor.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1398	Could not determine what version of service processor firmware is compatible with this version of the Hardware Management Console.	Check the version of your managed system and the HMC version first with Administration staff. Then determine the compatibility from the document, if they do match.
HSCL1399	The managed system does not have Virtual IO Server capability.	There is no recovery action necessary.

HSCL14xx error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCL14xx error codes	Message	Recovery action
HSCL1400	The firmware operation failed.	Try the task again. If the problem persists, contact your next level of support or your service provider.
HSCL1401	An error was detected using the current HMC's network configuration. A duplicate IP address and system hostname may be the cause of this problem. Verify this system's network settings via the 'Customize Network Settings' task. This HMC's network interface has been temporarily disabled and the hostname set to 'localhost.localdomain'.	<ol style="list-style-type: none">1. Ensure that the network setting is correct.2. If the problem persists, contact your next level of support or your service provider.
HSCL1402	This operation failed due to following reasons: {0}.	
HSCL1403	Could not display the {0} dialog. Try the operation again.	<ol style="list-style-type: none">1. Refresh the graphical user interface. For details, see Updating managed system or frame information.2. Retry the operation.3. If it still fails, log off and then log back in to the HMC and try the operation again.4. If the problem persists, contact your next level of support or your service provider.
HSCL1450	There is an insufficient number of unallocated processors to perform the operation.	<ol style="list-style-type: none">1. Rebuild the managed system. For details, see Updating managed system or frame information.2. Retry the task.3. If the problem persists, contact your next level of support or your service provider.
HSCL1451	Attempted to allocate a number of processors below the minimum processor setting.	<ol style="list-style-type: none">1. Ensure that the setting is valid.2. Retry the task.3. If the problem persists, contact your next level of support or your service provider.
HSCL1452	Attempted to allocate a number of processors above the maximum processor setting.	<ol style="list-style-type: none">1. Ensure that the setting is valid.2. Retry the task.3. If the problem persists, contact your next level of support or your service provider.
HSCL1453	There is an insufficient amount of unallocated processing units to perform the operation.	<ol style="list-style-type: none">1. Rebuild the managed system. For details, see Updating managed system or frame information.2. Retry the task.3. If the problem persists, contact your next level of support or your service provider.

HSCL14xx error codes	Message	Recovery action
HSCL1454	Attempted to allocate an amount of processing units below the minimum processing unit setting.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1455	Attempted to allocate an amount of processing units above the maximum processing setting.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1456	The processor setting exceeds the maximum system configuration.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1457	There is an insufficient amount of unallocated memory to perform the operation.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1458	Attempted to allocate an amount of memory below the minimum memory setting.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1459	Attempted to allocate an amount of memory above the maximum memory setting.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL145A	The minimum memory amount is below the required amount of memory with the maximum specified.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL145B	There is an insufficient amount of unallocated 5250 CPW to perform the operation.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL145C	Attempted to allocate an amount of 5250 CPW below the minimum setting.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL145D	Attempted to allocate an amount of 5250 CPW above the maximum setting.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.

HSCL14xx error codes	Message	Recovery action
HSCL145E	Attempted to allocate processing units greater than the maximum capacity allowed with the specified virtual processor setting.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL145F	Attempted to allocate processing units less than the minimum capacity allowed with the specified virtual processor setting.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1460	Attempted to set maximum processing units greater than the maximum capacity allowed with the specified virtual processor setting.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1461	Attempted to set maximum processing units less than the minimum capacity allowed with the specified virtual processor setting.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1462	Attempted to set minimum processing units greater than the maximum capacity allowed with the specified virtual processor setting.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1463	Attempted to set minimum processing units less than the minimum capacity allowed with the specified virtual processor setting.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1464	The partition is not currently configured for shared processing.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1465	The partition is not currently configured for dedicated processing.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1466	The partition specified is not valid. Rebuild the managed system and try again.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.

HSCL14xx error codes	Message	Recovery action
HSCL1467	The type of partition specified is not compatible with the operation.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1468	The I/O pool ID specified is not valid.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1469	The shared processor pool ID specified is not valid.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL146A	The I/O adapter: {0} is not valid.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL146B	The partition name specified has already been used by another partition. Specify a different name.	
HSCL146C	The partition name specified is not acceptable. Check the name and try again.	
HSCL146D	The partition is currently in a state where this configuration change is not allowed. Rebuild the managed system and try again.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL146E	The number of power controlling partitions for this partition is not valid. Check the setting and try again.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL146F	Changing from shared to dedicated processing is not allowed with the current processing setting.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1472	The SNI adapter: {0} specified is not valid. Check the entry and try again.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1473	Cannot perform atomic operation. Atomic operations are not enabled.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.

HSCL14xx error codes	Message	Recovery action
HSCL1474	The processing weight specified is not valid. Check the entry and try again.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1475	Unable to switch out or into manufacturing default configuration at this point.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1477	Unable to perform atomic operation(s) at this point since one is already in progress.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1478	The virtual I/O adapter type specified is not valid. Check the entry and try again.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1479	The atomic operation failed.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL147A	The RIO bus number: {0} is not valid. Check the entry and try again.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL147B	The hardware page table ratio specified is not valid. Check the entry and try again.	<ol style="list-style-type: none"> 1. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL147C	The I/O adapter: {0} cannot be assigned to the pool specified.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL147D	Cannot change the processing setting to uncapped.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL147E	The OptiConnect pool specified is not acceptable by the managed system. Check the entry and try again.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL147F	The HSL OptiConnect pool specified is not acceptable by the managed system. Check the entry and try again.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.

HSCL14xx error codes	Message	Recovery action
HSCL1481	Cannot perform this operation because the partition belongs to a workload management group joined by other partitions.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.

HSCL15xx CIMOM error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCL15xx error codes	Message	Recovery action
HSCL150B	Cannot change the I/O pools of the partition since the partition is still using an I/O adapter participating in one of the pool IDs.	
HSCL150C	Cannot use the I/O adapter: {0} since the partition is not part of the pool this adapter belongs to.	
HSCL150D	Cannot use the I/O adapter: {0} because it is not available.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL150E	Cannot use the I/O adapter: {0} since it is configured under an I/O unit marked as switchable.	
HSCL150F	Cannot vary off the I/O adapter: {0} because it is still in use by the partition.	
HSCL1510	This I/O adapter is marked as multi-hub reserving for shark partition.	
HSCL1511	Cannot use the I/O adapter: {0} because it is either used by another partition or an allocation is already in progress.	
HSCL1512	Cannot vary off the I/O adapter: {0} because the partition is not ready to release the adapter	
HSCL1513	Cannot change the OptiConnect setting since the communication with the partition is still active.	
HSCL1514	The virtual I/O slot number specified is not valid.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1515	Cannot use a virtual slot number greater or equal to the maximum number of virtual slots allowed with this partition.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.

HSCL15xx error codes	Message	Recovery action
HSCL1516	Cannot specify additional virtual LAN IDs since this virtual Ethernet adapter is not IEEE compatible.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1517	The virtual slot number specified to query or set virtual slot information is not valid.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1518	The virtual slot state specified is not valid.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1519	The number of virtual slots specified is not valid.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL151A	A virtual Ethernet trunk adapter with the same MAC address already exists.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL151B	Unable to delete the partition when there is a virtual terminal connection opened.	<ol style="list-style-type: none"> 1. Close the terminal session for the partition you want to delete. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL151C	Server adapter setting of the virtual slot: {0} is not valid.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL151D	The virtual adapter: {0} cannot be set up for HMC connection.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL151E	Cannot have multicast MAC address for the virtual Ethernet trunk adapter.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1523	Shared pool ID specified is not valid.	<ol style="list-style-type: none"> 1. Ensure that the setting is valid. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.

HSCL15xx error codes	Message	Recovery action
HSCL152A	Cannot change the managed system from the manufacturing default configuration because a partition is running with a device that does not support extended error handling (EEH).	
HSCL152D	The managed system is not ready for the Hardware Management Console to extract partition and resource information.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1537	The partition is not responsive for dynamic resource configuration changes.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1538	There is an insufficient amount of memory for maintaining system firmware.	
HSCL1539	Memory configuration for the partition cannot be satisfied due to system memory usage limitation.	
HSCL1550	Firmware command: {0} failed due to the following {1} errors: {2}	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1551	The firmware extended error code is {0}.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1552	The firmware operation failed with extended error.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1553	This operation cannot be performed because there is an insufficient number of unallocated processors for the i5/OS partitions.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1554	This operation cannot be performed because there is an insufficient number of unallocated processing units for the i5/OS partitions.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1555	The virtual I/O adapter configuration is not valid. If the remote partition and the remote partition virtual slot number are configured, make sure they are not the same number as the partition number and slot number of the virtual I/O adapter.	

HSCL15xx error codes	Message	Recovery action
HSCL1556	The virtual I/O adapter cannot be configured as a server adapter. The configuration is not allowed under the partition specified. The partition must be an i5/OS partition in an IBM System i5, eServer i5 system, or a virtual I/O server partition.	
HSCL157D	Unable to query the association within the managed system. Log in as the proper user and use the correct association method.	
HSCL157E	Unable to edit instance of {0}. Check user permissions, then log in as the proper user and try editing again.	<ol style="list-style-type: none"> 1. Check your user role's permissions. 2. If your user role does not permit the desired action, log out and log back in as the correct user, and retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL157F	Cannot find an instance of the object specified. Either there is no instance and it must be created or a path to the object was incorrect.	<ol style="list-style-type: none"> 1. Ensure that the inputs are correct. 2. Rebuild the managed system. For details, see Updating managed system or frame information. Then try the task again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1580	Improper number of arguments passed in: passed in = {0}, expected = {1}. Check the parameters of the invoked method.	<ol style="list-style-type: none"> 1. Verify that the command is being called correctly, and try the task again. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1581	The method name {0} passed in the invoke method does not match the name of the method you are trying to invoke. Check the method name and the required parameters.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1582	The wrong path is being used for the object manager - {0}. Check the code for build CIMObjectPath and its contents.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1583	The wrong object manager method is being invoked.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1584	You do not have the proper authorization or permission to perform this task. Log in as the proper user and try again.	Log in with appropriate permissions to perform the task. If the problem persists, contact your next level of support or your service provider.
HSCL1585	There was an unknown error while querying the object manager database.	<ol style="list-style-type: none"> 1. Try the task again. 2. Shut down and restart the HMC. 3. If the problem persists, contact your next level of support or your service provider.

HSCL15xx error codes	Message	Recovery action
HSCL1586	Cannot find an instance with object manager of {0}.	<ol style="list-style-type: none"> 1. Check the input. 2. Rebuild the managed system. For details, see Updating managed system or frame information. Then try the task again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1588	An exception was encountered while calling the method named {0}.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, rebuild the managed system. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL159B	The group number is invalid. Group numbers cannot contain any letters or characters other than the numbers 0 through 9.	Enter the new group number again without alphabetic characters.
HSCL159C	The Workload Management group number has to be between {0} and {1}.	Enter a number inside the valid range for workload management group numbers.
HSCL15E7	The profile you tried to activate does not belong to the partition {0} you specified. Select the correct partition profile.	Verify that you selected the correct logical partition profile to activate. If the operation still fails, contact your next level of support or your service provider.

HSCL17xx HMC console error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCL17xx error codes	Message	Recovery action
HSCL1771	Could not create console information and set it with the managed system. Perform the rebuild managed system operation.	Rebuild the managed system. For details, see Updating managed system or frame information.
HSCL1772	Could not set Hardware Management Console information. Perform the rebuild managed system operation.	Rebuild the managed system. For details, see Updating managed system or frame information.
HSCL1773	Invocation of the Hardware Management Console information method failed. Perform the rebuild managed system operation.	Rebuild the managed system. For details, see Updating managed system or frame information.
HSCL1774	Unable to get the defined slot number for Hardware Management Console information slots. Perform the rebuild managed system operation.	Rebuild the managed system. For details, see Updating managed system or frame information.
HSCL1776	Could not get the Hardware Management Console information. Perform the rebuild managed system operation.	Rebuild the managed system. For details, see Updating managed system or frame information.

HSCL17xx error codes	Message	Recovery action
HSCL1777	Failed to construct the Hardware Management Console information string. Perform the rebuild managed system operation.	Rebuild the managed system. For details, see Updating managed system or frame information.
HSCL1778	Could not create the Hardware Management Console instance in the object manager. Restart the Hardware Management Console.	<ol style="list-style-type: none"> 1. Restart the HMC. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1779	Could not create the Hardware Management Console motherboard instance in the object manager. Restart the Hardware Management Console.	<ol style="list-style-type: none"> 1. Restart the HMC. 2. If the problem persists, contact your next level of support or your service provider.
HSCL177A	Could not create the Hardware Management Console chassis instance in the object manager. Restart the Hardware Management Console.	<ol style="list-style-type: none"> 1. Restart the HMC. 2. If the problem persists, contact your next level of support or your service provider.
HSCL177B	Could not create the Hardware Management Console network setting instance in the object manager. Restart the Hardware Management Console.	<ol style="list-style-type: none"> 1. Restart the HMC. 2. If the problem persists, contact your next level of support or your service provider.
HSCL177C	Could not create the Hardware Management Console partition management instance in the object manager. Restart the Hardware Management Console.	<ol style="list-style-type: none"> 1. Restart the HMC. 2. If the problem persists, contact your next level of support or your service provider.
HSCL177D	Could not create the Hardware Management Console operating system instance in the object manager. Restart the Hardware Management Console.	<ol style="list-style-type: none"> 1. Restart the HMC. 2. If the problem persists, contact your next level of support or your service provider.
HSCL177E	Could not create the Hardware Management Console memory instance in the object manager. Restart the Hardware Management Console.	<ol style="list-style-type: none"> 1. Restart the HMC. 2. If the problem persists, contact your next level of support or your service provider.
HSCL177F	Could not delete the Hardware Management Console instance.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Shut down and restart the HMC and then try the task again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1780	Could not delete Hardware Management Console and its related instances.	<ol style="list-style-type: none"> 1. Restart the HMC. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1781	Could not obtain Hardware Management Console's VPD information. Restart the Hardware Management Console.	<ol style="list-style-type: none"> 1. Restart the HMC. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1782	Could not delete the Hardware Management Console Motherboard instance and its associations.	<ol style="list-style-type: none"> 1. Restart the HMC. 2. If the problem persists, contact your next level of support or your service provider.

HSCL17xx error codes	Message	Recovery action
HSCL1783	Could not delete the Hardware Management Console chassis instance and its associations.	<ol style="list-style-type: none"> 1. Restart the HMC. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1784	Could not delete the Hardware Management Console network setting instance and its associations.	<ol style="list-style-type: none"> 1. Restart the HMC. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1785	Could not delete the Hardware Management Console partition management instance and its associations.	<ol style="list-style-type: none"> 1. Restart the HMC. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1786	Could not delete the Hardware Management Console operating systems instance and its associations.	<ol style="list-style-type: none"> 1. Restart the HMC. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1787	Could not delete the Hardware Management Console memory instance and its associations.	<ol style="list-style-type: none"> 1. Restart the HMC. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1788	HMC information data has exceeded the 256 characters limit. Reduce the length of your host name.	

HSCL19xx WEBSM/AUIML error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

Back to HSCL error codes page

HSCL19xx error codes	Message	Recovery action
HSCL1965	Unable to determine the Hardware Management Console (HMC) server's host name. Check the HMC network settings under System Configuration and verify that they are correct.	<ol style="list-style-type: none"> 1. Check the HMC Network Settings under System Configuration to verify that the settings are correct and that you have a valid host name for the HMC. 2. Contact your system or network administrator for network settings help.
HSCL1967	You must select one system profile to power on with or select Cancel.	Select a system profile from the window or select Cancel to close the window.
HSCL1969	Could not retrieve information from the GUI server. Check your network configuration and connection.	Check the HMC network settings under System Configuration and verify that the settings are correct. If the problem persists, contact your next level of support or your service provider.
HSCL196A	Choose a new default profile from the list or select Cancel.	<ol style="list-style-type: none"> 1. Choose only one new default profile. 2. Either choose a new default profile, or select Cancel. 3. If the problem persists, contact your next level of support or your service provider.

HSCL19xx error codes	Message	Recovery action
HSCL196B	The object is not found in the data area. Refresh the interface.	<ol style="list-style-type: none"> 1. Perform the refresh task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL196C	Problem obtaining object information. Refresh the interface.	<ol style="list-style-type: none"> 1. Perform the refresh task. 2. If the same error occurs, perform the rebuild managed system operation. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL196E	Could not display the Operating System Shut down dialog. Try the operation again.	<ol style="list-style-type: none"> 1. Refresh the graphical user interface. For details, see Updating managed system or frame information. 2. Retry the operation. 3. If it still fails, log off and then log back in to the HMC and try the operation again. 4. If the problem persists, contact your next level of support or your service provider.
HSCL1970	Parent {0} name space not set.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Restart the HMC and try the task again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1971	There was an error retrieving necessary information from the Hardware Management Console. Refresh the console and try the operation again.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Restart the HMC and try the task again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1975	The HMC Access Password has been set from another HMC or ASM screen before this Update Password task completed. You must cancel out of the Update Password - Authentication Pending dialog and reselect this managed object to proceed.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the managed system state remains in <i>Pending Authentication</i>, restart the HMC and try the task again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1976	The ASM General Password has been set from another HMC or ASM screen before this Update Password task completed. You must cancel out of the Update Password - Authentication Pending dialog and reselect this managed object to proceed.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Restart the HMC and try the task again. 3. If the problem persists, contact your next level of support or your service provider.

HSCL19xx error codes	Message	Recovery action
HSCL1977	The ASM Administrator Password has been set from another HMC or ASM screen before this Update Password task completed. You must cancel out of the Update Password - Authentication Pending dialog and reselect this managed object to proceed.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Restart the HMC and try the task again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1978	An error occurred while attempting to update the HMC Access Password. Try to update the password again by either entering it again here or by cancelling out of this dialog and reselecting this managed system and its Update Managed System Password task.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1979	An error occurred while attempting to update the ASM General Password. Try to update the password again by either entering it again here or by cancelling out of this dialog and reselecting this managed system and its Update Managed System Password task.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL197A	An error occurred while attempting to update the ASM Administrator Password. Try to update the password again by either entering it again here or by cancelling out of this dialog and reselecting this managed system and its Update Managed System Password task.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL197B	Failed to backup the profile data {0} to file: {1}.	<ol style="list-style-type: none"> 1. Refresh the graphical user interface. For details, see Updating managed system or frame information. 2. Retry the task. 3. Restart the HMC, then try the task again. 4. If the problem persists, contact your next level of support or your service provider.
HSCL197C	Failed to remove backup file {0} from Managed System: {1}.	<ol style="list-style-type: none"> 1. Refresh the graphical user interface. For details, see Updating managed system or frame information. 2. Retry the task. 3. Restart the HMC, then try the task again. 4. If the problem persists, contact your next level of support or your service provider.
HSCL197D	Failed to initialize profile data at Managed System: {0}.	<ol style="list-style-type: none"> 1. Refresh the graphical user interface. For details, see Updating managed system or frame information. 2. Ensure that the operation was performed and that it displays on the graphical user interface. 3. If not, repeat the operation. 4. If the problem persists, contact your next level of support or your service provider.

HSCL19xx error codes	Message	Recovery action
HSCL197E	Failed to restore Managed System {0} from backup file {1} with {2}.	<ol style="list-style-type: none"> 1. Refresh the graphical user interface. For details, see Updating managed system or frame information. 2. Retry the task. 3. Rebuild the managed system. For details, see Updating managed system or frame information. 4. Retry the task. 5. If the problem persists, contact your next level of support or your service provider.
HSCL1980	Failed to copy profile: {0}.	<ol style="list-style-type: none"> 1. Try the task again. 2. Rebuild the managed system. For details, see Updating managed system or frame information. 3. Retry the operation. 4. If the problem still persists, contact your next level of support or your service provider.
HSCL1982	Profile Property Display failed. Exception: {0}.	<ol style="list-style-type: none"> 1. Refresh the graphical user interface. For details, see Updating managed system or frame information. 2. Retry the task. 3. Rebuild the managed system. For details, see Updating managed system or frame information. 4. Retry the task. 5. If the problem persists, contact your next level of support or your service provider.
HSCL1985	The following error(s) occurred during the operating system shut down of partition {0}: {1}.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL1986	There was an unknown error while changing the default profile.	<ol style="list-style-type: none"> 1. Try the task again. 2. Rebuild the managed system. For details, see Updating managed system or frame information. 3. Retry the operation. 4. If the problem still persists, contact your next level of support or your service provider.
HSCL198A	<p>No objects were found in the database. Possible problems and solutions are:</p> <ol style="list-style-type: none"> 1. The database is currently being populated. The object(s) should appear automatically when the database is fully populated, or you can retry later by clicking on Reload. 2. There is a problem with the connection between the Console and the Managed System. Ensure the network is correctly configured between the Console and the Managed System. 	<ol style="list-style-type: none"> 1. Ensure the network is correctly configured. 2. Restart the HMC 3. If the problem persists, contact your next level of support or your service provider.

HSCL19xx error codes	Message	Recovery action
HSCL198B	Failed to delete the selected profile(s).	<ol style="list-style-type: none"> 1. Try the task again. 2. Rebuild the managed system. For details, see Updating managed system or frame information. 3. Retry the operation. 4. If the problem still persists, contact your next level of support or your service provider.
HSCL198C	Failed to refresh the GUI for the deletion of the profile.	<ol style="list-style-type: none"> 1. Refresh the graphical user interface. For details, see Updating managed system or frame information. 2. Verify that the profile is deleted. 3. If the problem still persists, contact your next level of support or your service provider.
HSCL198D	The New HMC Access Password and Verify HMC Access Password do not match. Enter matching passwords to proceed.	Enter matching passwords.
HSCL198E	The New ASM General Password and Verify ASM General Password do not match. Enter matching passwords to proceed.	Enter matching passwords.
HSCL198F	The New ASM Administrator Password and Verify ASM Administrator Password do not match. Enter matching passwords to proceed.	Enter matching passwords.
HSCL1990	You have entered an incorrect password. Either the current HMC Access password specified is incorrect, or the HMC Access password has been changed already at another HMC and the New HMC Access password you specified here is wrong. Correct the password(s), then select OK once again from this dialog to retry the operation.	Enter the correct HMC Access password.
HSCL1991	The HMC Access Password you specified is incorrect. Enter the correct HMC Access Password to login.	Enter the correct HMC Access password.
HSCL1992	The HMC Access Password specified is invalid. The new password must be at least {0} and no greater than {1} characters in length. Enter the new password again to proceed.	Re-enter a password that conforms to the password rules.
HSCL1993	The ASM General Password specified is invalid. The new password must be at least {0} and no greater than {1} characters in length. Enter the new password again to proceed.	Re-enter a password that conforms to the password rules.
HSCL1994	The ASM Administrator Password specified is invalid. The new password must be at least {0} and no greater than {1} characters in length. Enter the new password again to proceed.	Re-enter a password that conforms to the password rules.

HSCL19xx error codes	Message	Recovery action
HSCL1995	<p>Your attempt to update the {0} password(s) has failed, because a successful attempt to update these passwords has taken place elsewhere during the time that has elapsed since this HMC last connected to the managed system. A reconnection to the managed system has been initiated to reset the password status, and the managed system state will be updated to reflect the true authentication state once this has completed. Note that none of the passwords stored on the managed system are what you attempted to set them to in this dialog.</p>	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the managed system state remains in <i>Pending Authentication</i>, restart the HMC and try the task again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1996	<p>Your attempt to update the {0} password(s) has succeeded. However, your attempt to update the {1} password(s) has failed because an update on this (these) password(s) has already happened successfully elsewhere during the time that has elapsed since this HMC last connected to the managed system.</p> <p>A reconnection to the managed system has been initiated to reset the password status, and the managed system state will be updated to reflect the true authentication state once this has completed. Note that for the failure cases, the password(s) stored on the managed system are not what you attempted to set them to in this dialog.</p>	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the managed system state remains in <i>Pending Authentication</i>, restart the HMC and try the task again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1997	<p>Your attempt to update the {0} password(s) has failed, because a successful attempt to update these passwords has taken place elsewhere during the time that has elapsed since this HMC last connected to the managed system. A subsequent attempt to reconnect to the managed system and reset the authentication state has also failed. 'Exit the Update Password - Pending Authentication dialog and retry the connection reset operation by selecting the 'Reset or Remove Connection' managed system task. If the problem persists, contact support.</p>	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the managed system state remains in <i>Pending Authentication</i>, restart the HMC and try the task again. 3. If the problem persists, contact your next level of support or your service provider.

HSCL19xx error codes	Message	Recovery action
HSCL1998	Your attempt to update the {0} password(s) has passed. However, your attempt to update the {1} password(s) has failed, because an update on this (these) passwords has already happened successfully elsewhere during the time that has elapsed since this HMC last connected to the managed system. A subsequent attempt to reconnect to the managed system and reset the authentication state has also failed. Exit the Update Password - Pending Authentication dialog and retry the connection reset operation by selecting the 'Reset or Remove Connection' managed system task. If the problem persists, contact support.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the managed system state remains in <i>Pending Authentication</i>, restart the HMC and try the task again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL1999	Your attempt to update the {0} password(s) has failed, because a successful attempt to update these passwords has taken place elsewhere during the time that has elapsed since this HMC last connected to the managed system. A reconnection to the managed system will be initiated to reset the password status once you exit this dialog, and the managed system state will be updated to reflect the true authentication state once this has completed. Note that none of the passwords stored on the managed system are what you attempted to set them to in this dialog.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the managed system state remains in <i>Pending Authentication</i>, restart the HMC and try the task again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL199A	Your attempt to update the {0} password or passwords has succeeded. However, your attempt to update the {1} password or passwords has failed, because an update has already happened successfully elsewhere during the time that has elapsed since this HMC last connected to the managed system. A reconnection to the managed system will be initiated to reset the password status once you exit this dialog, and the managed system state will be updated to reflect the true authentication state once this has completed. Note that for the failure cases, the password or passwords stored on the managed system are not what you attempted to set them to in this dialog.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the managed system state remains in <i>Pending Authentication</i>, restart the HMC and try the task again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL199B	The HMC Access Password specified is invalid. The password must be at least {0} and no greater than {1} characters in length. Re-enter a password of the correct length in this field to proceed.	Re-enter a password that conforms to the password rules.

HSCL19xx error codes	Message	Recovery action
HSCL199C	The ASM General Password specified is invalid. The password must be at least {0} and no greater than {1} characters in length. Re-enter a password of the correct length in this field to proceed.	Re-enter a password that conforms to the password rules.
HSCL199D	The ASM Administrator Password specified is invalid. The password must be at least {0} and no greater than {1} characters in length. Re-enter a password of the correct length in this field to proceed.	Re-enter a password that conforms to the password rules.
HSCL199E	An error occurred while trying to open the 5250 console. The error code is {0}. Contact your service provider.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL199F	An error occurred while trying to open the 5250 console. The error code is {0}. The additional data is {1}. Contact your service provider.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL19A0	An error occurred while trying to open the 5250 console. The operation timed out. The time out value used was {0} seconds. Try the operation again. If the problem persists, contact your service provider.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL19A1	An error occurred while trying to open the 5250 console. Try the operation again. If the problem persists, contact your service provider.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL19A2	Failed to save profile: {0}.	The Save profile command has failed. This operation cannot be done when the partition is either not bootable or has not been booted for the first time. You might try to activate the partition with an appropriate profile, or rebuild the managed system. Rebuild the managed system. For details, see Updating managed system or frame information.

HSCL24xx

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCL24xx error codes	Message	Recovery action
HSCL2400	The command failed during an HCA related operation.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Repeat the operation. 3. If the problem persists, contact your next level of support or your service provider.

HSCL24xx error codes	Message	Recovery action
HSCL2401	The specified HCA data {0} is not valid because it has been assigned to the profile already. Please select another adapter or remove the current assignment of the adapter and retry the operation.	<ol style="list-style-type: none"> 1. Only one GUID per adapter can be assigned to a logical partition. Make sure the new adapter has not been assigned already. 2. If the problem persists, contact your next level of support or your service provider.
HSCL2402	The specified HCA data {0} is not valid for the operation. Either the adapter ID or GUID does not exist, the resource capability is not valid, or the data is not in the format 'Adapter ID/GUID/Capabilities'. Please correct and retry the operation.	<ol style="list-style-type: none"> 1. If you were using the command line, verify the HCA data input to make sure the adapter ID, GUID, and Cap value are correct. 2. If you were using the HMC window, rebuild the system. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL2403	i5/OS logical partitions do not support HCA adapter in this release. Please remove the HCA adapter and retry the operation.	<ol style="list-style-type: none"> 1. HCA can only be assigned to RPA logical partitions. Remove the HCA assignment and retry the operation. 2. If the problem persists, contact your next level of support or your service provider.

HSCL25xx user management error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCL25xx error codes	Message	Recovery action
HSCL251D	There was an unknown internal Hardware Management Console error.	<ol style="list-style-type: none"> 1. Repeat the operation. 2. If it still fails, restart the HMC. 3. If the problem persists, contact your next level of support or your service provider.
HSCL251E	Failed to set the \enable remote virtual terminal\ option.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL251F	The following error was encountered: {0}. Retry the operation.	<ol style="list-style-type: none"> 1. Ensure the network connection between the HMC and the partition is working. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL2520	The command entered is not supported.	<ol style="list-style-type: none"> 1. Retry the task. 2. If the problem persists, contact your next level of support or your service provider.

HSCL25xx error codes	Message	Recovery action
HSCL2521	There was a failure in the HMC Repository.	<ol style="list-style-type: none"> 1. Restart the HMC, and retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL2522	The firmware command {0} failed. The return code from firmware is {1}.	<ol style="list-style-type: none"> 1. Try the task again. 2. If the problem persists, contact your next level of support or your service provider.
HSCL2523	A critical property, {0}, stored in the repository is not set.	<ol style="list-style-type: none"> 1. Rebuild the managed system, and try the task again. For details, see Updating managed system or frame information. 2. Restart the HMC, and retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL2524	Invalid subscription ID {0}	<ol style="list-style-type: none"> 1. Log off and then log back in to the HMC and try the operation again. 2. If the problem persists, contact your next level of support or your service provider.
HSCL2525	Authentication failed.	<ol style="list-style-type: none"> 1. Log off and then log back in to the HMC and try the operation again. 2. If the problem persists, contact your next level of support or your service provider.
HSCL2526	The following errors occurred during the {0} operation {1}	

HSCL29xx user management error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCL29xx error codes	Message	Recovery action
HSCL2901	This logical partition is not capable of adding, removing, or moving processors dynamically.	Ensure your logical partitions are capable of performing dynamic logical partition operations.
HSCL2902	The destination logical partition is not capable of adding, removing, or moving processors dynamically.	Ensure your logical partitions are capable of performing dynamic logical partition operations.
HSCL2903	Your processor request goes below the profile's required processor limit. You can remove or move {0} or fewer processors. Retry the operation.	Retry the operation, entering a smaller number of processors.
HSCL2904	Your processor request exceeds the profile's maximum processor limit. You can add or move up to {0} processors. Retry the operation.	Retry the operation, entering a smaller number of processors.
HSCL2905	This logical partition is not capable of adding, removing, or moving memory dynamically.	Ensure your logical partitions are capable of performing dynamic logical partition operations.

HSCL29xx error codes	Message	Recovery action
HSCL2906	The destination logical partition is not capable of adding, removing, or moving memory dynamically.	Ensure your logical partitions are capable of performing dynamic logical partition operations.
HSCL2907	Your memory request exceeds the profile's maximum memory limit. You can add or move up to {0} MBs of memory. Retry the operation.	<ol style="list-style-type: none"> 1. Retry the task and request a smaller memory amount. 2. Reset the logical partition, reactivate the logical partition, and then retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL2908	Your memory request goes below the profile's minimum memory limit. You can remove or move up to {0} MB of memory. Retry the operation.	<ol style="list-style-type: none"> 1. Retry the task and request a larger memory amount. 2. Reset the logical partition, reactivate the logical partition, and then retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL2909	Your memory request exceeds the total available memory of the managed system. You can add up to {0} MB of memory. Retry the operation.	<ol style="list-style-type: none"> 1. Check the available memory of the managed system, retry the task and request a smaller memory amount. 2. Reset the logical partition, reactivate the logical partition, and then retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL290B	This logical partition is not capable of adding, removing, or moving I/O slots dynamically.	Ensure your logical partitions are capable of performing dynamic logical partition operations.
HSCL290C	The destination logical partition is not capable of adding, removing, or moving I/O slots dynamically.	Ensure your logical partitions are capable of performing dynamic logical partition operations.
HSCL2912	The managed system is powered off. You must power on the managed system to perform a dynamic logical partition operation.	<ol style="list-style-type: none"> 1. Ensure the managed system is powered on. 2. Rebuild managed system. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL2914	The quantity to be added exceeds the available resources.	<ol style="list-style-type: none"> 1. Ensure that memory is available in the managed system. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL2916	The partition could not be found in the database. Perform a rebuild managed system operation, and try again.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL2925	An unknown error occurred during the add Virtual adapter operation. Retry the operation.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.

HSCL29xx error codes	Message	Recovery action
HSCL2926	An unknown error occurred during the remove Virtual adapter operation. Retry the operation.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL2927	Dynamic logical partition MOVE Processing resources failed: {0}.	<ol style="list-style-type: none"> 1. Retry the task. 2. Rebuild the managed system. For details, see Updating managed system or frame information. 3. Retry the task. 4. If the problem persists, contact your next level of support or your service provider.
HSCL2928	Dynamic logical partition ADD I/O resources failed: {0}.	<ol style="list-style-type: none"> 1. Ensure you have the resources available to perform the operation. 2. Retry the operation. 3. If operation still fails, rebuild the managed system and try the operation again. For details, see Updating managed system or frame information. 4. If the problem persists, contact your next level of support or your service provider.
HSCL2929	Dynamic logical partition REMOVE I/O resources failed: {0}.	<ol style="list-style-type: none"> 1. Ensure you have the resources available to perform the operation. 2. Retry the operation. 3. If operation still fails, rebuild the managed system and try the operation again. For details, see Updating managed system or frame information. 4. If the problem persists, contact your next level of support or your service provider.
HSCL2930	Dynamic logical partition MOVE I/O resources failed: {0}.	<ol style="list-style-type: none"> 1. Ensure you have the resources available to perform the operation. 2. Retry the operation. 3. If operation still fails, rebuild the managed system and try the operation again. For details, see Updating managed system or frame information. 4. If the problem persists, contact your next level of support or your service provider.
HSCL2931	Dynamic logical partition ADD Memory resources failed: {0}.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.

HSCL29xx error codes	Message	Recovery action
HSCL2932	Dynamic logical partition REMOVE Memory resources failed: {0}.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If it still fails, try increasing the value in the timeout setting field in the Advanced tab in the DLPAR window. Note: The default timeout is 5 minutes. You can change the value to a number greater than 5, or to a 0 to have the system take as long as necessary. 3. If the problem persists, contact your next level of support or your service provider.
HSCL2933	Dynamic logical partition MOVE Memory resources failed: {0}.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL2934	The operating system drmgr command failed. Consult the appropriate operating system log files for further information and retry the operation if desired.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL2935	{0} operation for {1} resource did not finish completely in the timeout value specified. The requested number was {2}. The success number is {3}. Increase the timeout value if needed.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL2936	{0} operation for {1} resource failed.	<ol style="list-style-type: none"> 1. Ensure the network connection between the HMC and the logical partition is working. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL2937	{0} operation for {1} has completed, but only {3} out of {2} were successful. The partition standard output/error is not available.	
HSCL2938	{0} operation for {1} resource failed. The RPA partition standard output/error is not available.	
HSCL2939	{0} operation for {1} has completed, but only {3} out of {2} were successful. The partition standard output is: {4}. The AIX standard error is: {5}.	
HSCL293A	{0} operation for {1} has completed, but only {3} out of {2} were successful. The partition command is: {4}. The partition standard output is: {5} The partition standard error is: {6}.	
HSCL293B	The return code is {0}. The partition return code is {1}.	
HSCL293D	Partition {0} is not in the correct state to perform dynamic logical partitioning operations.	<p>Dynamic logical partitioning operations can only be performed on running partitions.</p> <ol style="list-style-type: none"> 1. Verify that the partition is in the Running state, and retry the operation. 2. If the problem persists, contact your next level of support or your service provider.

HSCL29xx error codes	Message	Recovery action
HSCL2940	An unknown Dynamic logical partition error has occurred. Try the operation again.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL2941	There are no processors available for dynamic logical partitioning on this partition.	<ol style="list-style-type: none"> 1. Ensure that there are available processors in the managed system. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL2942	There is no memory available for dynamic logical partitioning on this partition.	<ol style="list-style-type: none"> 1. Ensure that there are available processors in the managed system. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL2944	The I/O slot cannot be found. Ensure that the correct slot ID and unit ID were entered.	<ol style="list-style-type: none"> 1. Ensure the inputs are correct. 2. Rebuild managed system. For details, see Updating managed system or frame information. 3. Retry the task. 4. If the problem persists, contact your next level of support or your service provider.
HSCL2945	The shut down operation on the logical partition failed. The return code is {0}.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL2946	The logical partition could not be shut down because the HMC's communication to the partition failed. The return code is {0}.	<ol style="list-style-type: none"> 1. Ensure the network connection between the partition and the HMC is working. 2. Restart the HMC and retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL2947	An error occurred while trying to restore stopped processors. There were {0} processors restored before the error occurred.	
HSCL2949	An error occurred while trying to restore stopped I/O devices. There were {0} devices restored before the error occurred.	
HSCL294A	The I/O slot cannot be found or it is required. Ensure that the valid slot ID and unit ID were entered.	<ol style="list-style-type: none"> 1. Ensure the inputs are correct. 2. Ensure the adapter is not marked as required. 3. Rebuild the managed system. For details, see Updating managed system or frame information. 4. If the problem persists, contact your next level of support or your service provider.
HSCL294C	Dynamic logical partition ADD Virtual I/O resources failed: {0}.	<ol style="list-style-type: none"> 1. Correct the error and retry the operation. 2. If the problem persists, contact your next level of support or your service provider.

HSCL29xx error codes	Message	Recovery action
HSCL294D	Dynamic logical partition REMOVE Virtual I/O resources failed: {0}.	<ol style="list-style-type: none"> 1. Correct the error and retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL294E	Dynamic logical partition ADD Processing resources failed: {0}.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If operation still fails, perform a Rebuild Managed System operation, and try the operation again. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL294F	Dynamic logical partition REMOVE Processing resources failed: {0}.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If operation still fails, perform a Rebuild Managed System operation, and try the operation again. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL2950	Dynamic logical partition operation on PCI Host Bridge failed.	<ol style="list-style-type: none"> 1. Ensure you have the resources available to perform the operation. 2. Retry the operation. 3. If operation still fails, perform a Rebuild Managed System operation, and try the operation again. For details, see Updating managed system or frame information. 4. If the problem persists, contact your next level of support or your service provider.
HSCL2952	The dynamic logical partitioning requested could not be completed due to an unknown error(s) in the local system. Retry the operation.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL2957	There is currently no RMC connection between the HMC and the RPA partition {0}. This could be because the partition is inactive, a firewall, or an improper network setup causing RMC not to recognize the partition. Please check the system network setup.	<ol style="list-style-type: none"> 1. Ensure that the network connection is working between HMC and the partition. For details, see "Task 4. Ensure that your physical networking is set up correctly" on page 86. 2. If the problem persists, contact your next level of support or your service provider.

HSCL29xx error codes	Message	Recovery action
HSCL2965	DLPAR ADD Processing resources failed. The requested number of processors to be added exceeds the number of processors that are currently available for i5/OS partitions: {0} processors are currently available.	<ol style="list-style-type: none"> 1. If there are processors currently available for i5/OS partitions, reduce the requested number of processors to be added to be less than or equal to that number. 2. Alternatively, shut down other i5/OS partitions or use Dynamic Logical Partitioning to remove processing resources from other i5/OS partitions to release enough processors. Note that the number of i5/OS processors in use by an uncapped i5/OS partition is equivalent to the number of virtual processors in use by that partition. Therefore, in order to release i5/OS processors from an uncapped i5/OS partition, you must release virtual processors from that partition. Releasing one virtual processor from an uncapped i5/OS partition will release one physical i5/OS processor. 3. Try the task again.
HSCL2966	DLPAR ADD Processing resources failed. The requested number of processing units to be added exceeds the number of processing units that are currently available for i5/OS capped partitions: {0} processing units are currently available.	<ol style="list-style-type: none"> 1. If there are processing units currently available for i5/OS capped partitions, reduce the requested number of processing units to be added to be less than or equal to that number. 2. Alternatively, shut down other i5/OS partitions or use Dynamic Logical Partitioning to remove processing resources from other i5/OS partitions to release enough processing units. Note that the number of i5/OS processing units in use by an uncapped i5/OS partition is equivalent to the number of virtual processors in use by that partition. Therefore, in order to release i5/OS processing units from an uncapped i5/OS partition, you must virtual processors from that partition. Releasing one virtual processor from an uncapped i5/OS partition will release one physical i5/OS processing unit. 3. Try the task again.
HSCL2967	DLPAR ADD Processing resources failed. The requested number of virtual processors to be added exceeds the number of virtual processors that are currently available for i5/OS uncapped partitions: {0} virtual processors are currently available.	<ol style="list-style-type: none"> 1. If there are virtual processors currently available for i5/OS uncapped partitions, reduce the requested number of virtual processors to be added to be less than or equal to that number. 2. Alternatively, shut down other i5/OS partitions or use Dynamic Logical Partitioning to remove processing resources from other i5/OS partitions to release enough virtual processors. To add one virtual processor to an uncapped i5/OS partition, one physical i5/OS processor must be available. 3. Try the task again.

HSCL29xx error codes	Message	Recovery action
HSCL2968	DLPAR MOVE Processing resources failed. The requested number of processors cannot be moved to the i5/OS partition {0} because doing so would cause the i5/OS processor capacity limit of {1} processors for this managed system to be exceeded.	<ol style="list-style-type: none"> 1. If possible, reduce the requested number of processors to be moved to the i5/OS partition, and try the task again. 2. Alternatively, move processing resources from other i5/OS partitions to this partition. 3. Alternatively, shut down other i5/OS partitions to release i5/OS processors. Note that the number of i5/OS processors in use by an uncapped i5/OS partition is equivalent to the number of virtual processors in use by that partition. Therefore, shutting down an uncapped i5/OS partition will release one physical i5/OS processor for each virtual processor assigned to that partition.
HSCL2969	DLPAR MOVE Processing resources failed. The requested number of processing units cannot be moved to the i5/OS partition {0} because doing so would cause the i5/OS processor capacity limit of {1} processing units for this managed system to be exceeded. Up to {2} processing units can be moved from partition {3} to partition {0}.	<ol style="list-style-type: none"> 1. If possible, reduce the requested number of processing units to be moved to the i5/OS partition, and try the task again. 2. Alternatively, move processing resources from other i5/OS partitions to this partition. 3. Alternatively, shut down other i5/OS partitions to release i5/OS processing units. Note: The number of i5/OS processing units in use by an uncapped i5/OS partition is equivalent to the number of virtual processors in use by that partition. Therefore, shutting down an uncapped i5/OS partition will release one physical i5/OS processor.
HSCL296A	DLPAR MOVE Processing resources failed. The requested number of virtual processors cannot be moved to the i5/OS partition {0} because doing so would cause the i5/OS processor capacity limit of {1} processors for this managed system to be exceeded.	<ol style="list-style-type: none"> 1. If possible, reduce the requested number of virtual processors to be moved to the i5/OS partition, and try the task again. 2. Alternatively, move processing resources from other i5/OS partitions to this partition. 3. Alternatively, shut down other i5/OS partitions to release i5/OS virtual processors. To move one virtual processor to an uncapped i5/OS partition, one physical i5/OS processor must be available.

HSCL29xx error codes	Message	Recovery action
HSCL296B	The i5/OS partition {0} cannot be changed to an uncapped partition because too many virtual processors are assigned to the partition. Reduce the number of virtual processors assigned to the partition and try again.	<ol style="list-style-type: none"> 1. Make sure that the maximum number of virtual processors defined for the partition is less than or equal to the i5/OS processor capacity limit for your managed system. If it is not, then reduce the maximum number of virtual processors defined in the partition's profile, and then reactivate the partition. Try the task again. 2. Use Dynamic Logical Partitioning to remove virtual processors from the partition until the total number of processing resources in use by all i5/OS partitions, including the number of virtual processors assigned to this partition, does not exceed the i5/OS processor capacity limit for your managed system. Note that the number of i5/OS processors in use by an uncapped i5/OS partition is equivalent to the number of virtual processors in use by that partition. 3. Alternatively, shut down other i5/OS partitions or use Dynamic Logical Partitioning to remove processing resources from other i5/OS partitions to release enough virtual processors for this partition. 4. Try the task again.
HSCL2970	The IOServer command has failed because of the following reason: {0}.	Retry the command. If the problem persists, contact your next level of support or your service provider.
HSCL2971	The IOServer command fails because the partition {0} is unknown to RMC/LparCmdRM. This could be because of a firewall or an improper network setup causing RMC not to recognize the partition. Check the system network setup.	This could be caused by a firewall or an incorrect network setup causing Resources Monitoring Control (RMC) not to recognize the partition. Check the system network setup.
HSCL2972	There is no active session between the HMC and the partition.	<ol style="list-style-type: none"> 1. There could be a short interruption in the network causing Resources Monitoring Control (RMC) to not recognize the partition. 2. Retry the operation later or restart the HMC. 3. If the problem persists, contact your next level of support or your service provider.
HSCL2973	The IOServer command contained illegal characters such as ; or >.	Illegal characters are in the IOServer command. Check the IOServer command to make sure it does not include illegal characters, and try the task again.
HSCL2974	The active profile includes all resources. You are not allowed to add, remove, or move resources from this configuration	No recovery action.
HSCL2975	The IOClient command has failed because of the following reason: {0}	No recovery action.

HSCL29xx error codes	Message	Recovery action
HSCL2976	The IOClient command fails because the partition {0} is unknown to RMC/LparCmdRM. This could be because the partition is inactive, or because a firewall or an improper network setup causing RMC not to recognize the partition. Please check the system network setup.	Check the system network setup.
HSCL2977	The IOClient command contains illegal characters such as ; or >.	No recovery action.
HSCL2978	The partition {0} is not in the Running state. First activate the partition and try the operation again.	Activate the partition and try the operation again.
HSCL2979	There was an error retrieving the Virtual IO connection status for the managed system. Execute a rebuild managed system operation. If the error persists contact your service service representative.	<ol style="list-style-type: none"> 1. Perform a rebuild of the managed system. For details, see Updating managed system or frame information. 2. Try the task again. 3. If the operation still fails, contact support.

HSCL3xxx error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCL3xxx error codes	Message	Recovery action
HSCL3006	The LED operation failed. Refer to the HMC Operations Guide for more details. {0}	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3060	The following managed frames failed to initialize: {0}. If the error persists, contact your software service representative.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3070	The Frame lock action failed. Try the operation again.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3071	The Frame Guided Maintenance operation failed. Try the operation again.	Try the operation again. If the problem persists, contact your hardware representative.
HSCL3072	The Frame FRU deactivation operation failed. Try the operation again.	Try the operation again. If the problem persists, contact your hardware representative.
HSCL3073	The Frame FRU activation operation failed. Try the operation again.	Try the operation again. If the problem persists, contact your hardware representative.
HSCL3074	The frame host information was not saved. Ensure the Hardware Management Console has enough disk space and the correct file permission and try the operation again.	Ensure that the /opt/hsc/data directory contains enough disk space so that the HMC can save the frame host information when needed.

HSCL3xxx error codes	Message	Recovery action
HSCL3075	The frame host information that was found is not valid. Check the host information you provided and try the operation again.	Check the frame host information that was entered into the application program to ensure the host name, password, and frame bulk power controller (BPC) internal identification are valid.
HSCL3076	An error has occurred while attempting the bulk power assembly connection operation. Retry the operation. If the problem persists, contact your service representative.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3077	This operation is not allowed in the frame's current state. In order for this operation to be performed, at least one bulk power assembly (BPA) must be in the Standby state.	<ol style="list-style-type: none"> 1. Make sure that at least one bulk power assembly is in the Standby state, and try the operation again. 2. If the problem persists, contact your hardware representative.
HSCL3078	The request to power on the drawer or planar for the frame failed. Try the request again.	Try the request again. If the problem persists, contact your service provider.
HSCL3079	The request to add a drawer to the frame failed. Try the request again.	Try the request again. If the problem persists, contact your service provider.
HSCL307A	This operation cannot be performed because the HMC is not connected to side {0} of the bulk power assembly (BPA). Check the connection and try the operation again.	<ol style="list-style-type: none"> 1. Check the connection. 2. Try the operation again. 3. If the problem persists, contact your next level of support or your service provider.
HSCL3080	The request to remove a planar from the frame failed. Try the request again.	Try the request again. If the problem persists, contact your next level of support or your service provider.
HSCL3081	The request to remove a drawer from the frame failed. Try the request again.	Try the request again. If the problem persists, contact your next level of support or your service provider.
HSCL3082	The request to send the frame IP information to the managed system has failed.	Try the request again. If the problem persists, contact your next level of support or your service provider.
HSCL3083	This operation is not allowed when the cage is powered on. Before this operation can be performed, all the cages must be powered off.	
HSCL3084	This operation is not allowed when the BPA is in any of the following states: Incomplete, No Connection, or Not Available. After you have established a connection from the HMC to the BPA, and have entered a valid HMC access password, try the operation again.	
HSCL3200	Unknown lock error.	Contact your next level of support or your service provider.
HSCL3201	Lock type not valid.	<ol style="list-style-type: none"> 1. Restart the HMC. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3202	Failed to acquire lock because of timeout.	<ol style="list-style-type: none"> 1. Restart the HMC. 2. If the problem persists, contact your next level of support or your service provider.

HSCL3xxx error codes	Message	Recovery action
HSCL3203	Nested lock type requested not valid.	<ol style="list-style-type: none"> 1. Restart the HMC. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3204	Lock not held.	<ol style="list-style-type: none"> 1. Restart the HMC. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3205	The managed system is busy, try the operation again later.	The managed system is busy doing another action. Wait and then retry the action.
HSCL3351	Code update process is not allowed by the HMC. Check the code update status to verify the code update owner.	<ol style="list-style-type: none"> 1. Check the code update status to verify the code update owner. 2. Retry the operation if HMC is the code update owner. 3. If the problem persists, contact your next level of support or your service provider.
HSCL3352	Code update is already in progress by another HMC or by the firmware. Verify that no other code update is in progress and retry the operation.	<ol style="list-style-type: none"> 1. Verify that no other code update operation is in progress and retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3353	Code update is not allowed to the specified side. Check the current flash side.	<ol style="list-style-type: none"> 1. Rebuild the managed operation. For details, see Updating managed system or frame information. 2. Check the power-on side from the managed system property panel and ensure you are not performing code update to the power-on side and then retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL3354	Code update is already in progress from this HMC. Ensure that no code update operation is in progress on the HMC before retrying the operation.	<ol style="list-style-type: none"> 1. Ensure that no code update operation is in progress on the HMC before retrying the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3355	The code update operation failed with return code {0}.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3356	The code update is not in progress by this HMC. The start code update task should have been performed prior to code update complete by this HMC.	<ol style="list-style-type: none"> 1. Ensure that the start code update task has been performed. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL3357	The operation failed since another commit or long running code update is in progress.	<ol style="list-style-type: none"> 1. Ensure that no other code update operation is in progress. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.

HSCL3xxx error codes	Message	Recovery action
HSCL3358	The delete LID operation is not allowed when a write LID is in progress.	<ol style="list-style-type: none"> 1. Ensure that no other code update operation is in progress. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL3359	The code update operation failed since an invalid LID ID was specified.	<ol style="list-style-type: none"> 1. Check the LID file ID and retry the operation with a valid LID file ID. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3360	Error accessing the flash.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3361	An unknown error occurred during code update operation. Retry the operation.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3362	An unknown error occurred during reboot service processor. Retry the operation.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3363	The size of the LID number array is not the same as the Filename array. Ensure every LID number has a corresponding filename.	<ol style="list-style-type: none"> 1. Ensure every LID number has a corresponding filename and retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3364	The read LID operation failed: {0}.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3365	Error: The following file(s) already exist(s): {0}.	<ol style="list-style-type: none"> 1. Ensure the files to read in the LID files do not exist and retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3367	The input parameter arrays should all be of the same length. Check the lengths and retry the operation.	<ol style="list-style-type: none"> 1. Ensure the lengths of the input parameters are the same and retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3368	The Max write block size for the start code update did not get set. Retry the operation.	<ol style="list-style-type: none"> 1. Retry the operation for the LID files that failed. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3370	The deletion of the following LID(s) failed: {0}.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3371	The write LID operation failed: {0}.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.

HSCL3xxx error codes	Message	Recovery action
HSCL3372	The following LID filenames are not files: {0}	<ol style="list-style-type: none"> 1. Ensure the LID files exist and retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3373	The following LID files are empty: {0}	<ol style="list-style-type: none"> 1. Ensure that the LID files are valid and retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3374	The following LID files do not exist: {0}	<ol style="list-style-type: none"> 1. Ensure the LID files exist and retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3376	Invalid value returned from the service processor to indicate whether service partition firmware code LID updates are enabled or disabled.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3377	The start code update operation failed since an invalid component to update was specified. Retry the operation with the a valid firmware component to update.	<ol style="list-style-type: none"> 1. Retry the operation with a valid firmware component to update. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3378	The start code update operation failed since the managed system is not in the valid state. Check the state of the managed system and retry the operation.	<ol style="list-style-type: none"> 1. Check the state of the managed system and retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3379	There is a permanent error in flash, retry the operation and if the problem persists contact support.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3380	The Code Update operation failed since the managed system is not in the Power Off, Operating, or Standby state. Check the managed system's state and retry the operation.	<ol style="list-style-type: none"> 1. Check the state of the managed system and retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3381	The Complete Code Update operation failed since an invalid completion type was specified. Retry the operation with a valid completion type.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3382	The Code Update is not in progress. The start code update operation needs to be performed before the Complete Code Update operation.	<ol style="list-style-type: none"> 1. Ensure the start code update operation is performed first. 2. Retry the operation. 3. If the problem persists, contact your next level of support or your service provider.
HSCL3383	One or more LIDs are invalid in the primary LID list.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3384	For the partial read, the specified length was not read since the end of file flag was reached.	<ol style="list-style-type: none"> 1. Retry the operation with a valid length to be read. 2. If the problem persists, contact your next level of support or your service provider.

HSCL3xxx error codes	Message	Recovery action
HSCL3385	Error: The following file(s) specified an invalid data for the Special LID Designator or the code update side: {0}	<ol style="list-style-type: none"> 1. Retry the operation with valid special LID designator or the code update side. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3386	The read partial/special LID operation failed, since writing to the file on the HMC got an error. Check the log for the error and retry the operation.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3387	An unknown error occurred during the open of firmware files. Retry the operation.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3388	The following fileid-subid specified an invalid open type: {0}	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3389	The following fileid-subid specified an invalid Force Flag: {0}	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3390	Error: The following files got an exception while trying to open the firmware file: {0}	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3391	The open firmware file operation failed: {0}	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3392	An unknown error occurred during the write operation of firmware files. Retry the operation.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3393	An unknown error occurred during the close of firmware files. Retry the operation.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3394	An unknown error occurred during the get firmware status update operation. Retry the operation.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3395	An unknown error occurred during the start firmware update operation. Retry the operation.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3396	Failed to delete the partition with ID {0} since it is the service partition.	<ol style="list-style-type: none"> 1. Ensure the partition is not the service partition. 2. Rebuild the managed system. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL3397	The secondary service processor is not available for the managed system.	<ol style="list-style-type: none"> 1. Check the FSP configuration and make sure that the service processor is installed and available for failover. 2. If the problem persists, contact your next level of support or your service provider.

HSCL3xxx error codes	Message	Recovery action
HSCL3398	The code update service processor lock is already taken. Check that no other code update operation is running and retry the operation.	<ol style="list-style-type: none"> 1. Check that no other code update operation is in progress and retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3399	The code update service processor lock is not taken. Ensure the lock is taken before trying to release the code update service processor lock.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3400	The service processor target that was specified is not valid. Verify the service processor target name and try the request again.	<ol style="list-style-type: none"> 1. Rebuild the managed frame. For details, see Updating managed system or frame information. 2. Try the task again. 3. If the problem persists, contact your service provider.
HSCL3401	The get power domain operation failed. Retry the operation.	<ol style="list-style-type: none"> 1. The I/O concurrent maintenance command failed. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3402	The get power domain power state operation failed. Retry the operation.	<ol style="list-style-type: none"> 1. The I/O concurrent maintenance command failed. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3403	The set service lock operation failed. Retry the operation.	<ol style="list-style-type: none"> 1. The I/O concurrent maintenance command failed. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3404	The reset service lock operation failed. Retry the operation.	<ol style="list-style-type: none"> 1. The I/O concurrent maintenance command failed. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3405	The FRU level activate operation failed. Retry the operation.	<ol style="list-style-type: none"> 1. The I/O concurrent maintenance command failed. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3406	The FRU level deactivate operation failed. Retry the operation.	<ol style="list-style-type: none"> 1. The I/O concurrent maintenance command failed. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3407	The vary off power domain platform operation failed. Retry the operation.	<ol style="list-style-type: none"> 1. The I/O concurrent maintenance command failed. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3408	The vary off power domain platform operation failed. Retry the operation.	<ol style="list-style-type: none"> 1. The I/O concurrent maintenance command failed. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.

HSCL3xxx error codes	Message	Recovery action
HSCL3409	The vary on power domain platform operation failed. Retry the operation.	<ol style="list-style-type: none"> 1. The I/O concurrent maintenance command failed. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3410	The vary off power domain partition operation failed. Retry the operation.	<ol style="list-style-type: none"> 1. The I/O concurrent maintenance command failed. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3411	The vary off power domain partition operation failed. Retry the operation.	<ol style="list-style-type: none"> 1. The I/O concurrent maintenance command failed. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3412	The vary on power domain partition operation failed. Retry the operation.	<ol style="list-style-type: none"> 1. The I/O concurrent maintenance command failed. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3413	No Partitions are defined for the managed system. Check the user interface to see if partitions are defined and then retry the operation.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task. 3. If the problem persists, contact your next level of support or your service provider.
HSCL3414	The start I/O concurrent maintenance operation failed. Retry the operation.	<ol style="list-style-type: none"> 1. The I/O concurrent maintenance command failed. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3415	The I/O concurrent maintenance operation failed. Retry the operation.	<ol style="list-style-type: none"> 1. The I/O concurrent maintenance command failed. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3416	The get configuration ID operation failed. Retry the operation.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3417	The set configuration ID operation failed. Retry the operation.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3418	The get IO unit configuration ID and MTMS operation failed. Retry the operation.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3419	The set IO unit MTMS operation failed. Retry the operation.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3420	The set IO unit configuration ID operation failed. Retry the operation.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.

HSCL3xxx error codes	Message	Recovery action
HSCL3421	This operation is not allowed in the managed system's current state. Check the state of the managed system and retry the operation.	<ol style="list-style-type: none"> 1. Check the state of the managed system and retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3422	This operation cannot be completed because a conflicting concurrent maintenance operation is already in progress. Ensure that the other operation has completed and then retry the operation.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3423	Invalid data {0} was specified for this operation. Check the data and retry the operation.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3424	The I/O concurrent maintenance operation failed with return code: {0}.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3431	The command display service effect failed {%0}. Please retry the operation again.	
HSCL3432	The system level deactivation failed {%0}. Please retry the operation.	
HSCL3433	The system level deactivation failed {%0}. Please retry the operation.	
HSCL3437	The managed system does not have Concurrent Maintenance capability. Please upgrade the firmware and retry the operation.	<ol style="list-style-type: none"> 1. Upgrade the firmware that supports Platform Hardware Concurrent Maintenance and retry the operation. For details, see "Obtaining firmware updates" on page 135. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3438	The managed system does not have PHYP Concurrent Maintenance capability. Please upgrade the firmware and retry the operation.	<ol style="list-style-type: none"> 1. Upgrade the firmware that supports Platform Hardware Concurrent Maintenance and retry the operation. For details, see "Obtaining firmware updates" on page 135. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3439	Query FSP CM Service Lock failed. Please retry the operation.	<ol style="list-style-type: none"> 1. Please retry the operation 2. If the problem persists, contact your next level of support or your service provider.
HSCL3500	The function completed successfully.	
HSCL3501	The operation failed because of a non-trivial reason.	<ol style="list-style-type: none"> 1. Restart the HMC and retry the task. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3503	Input error: The specified value is out of range or undefined.	Contact your next level of support or your service provider.
HSCL3504	An invalid input file or an error has occurred during an operation on the specified file.	<ol style="list-style-type: none"> 1. Restart the system. 2. If the problem persists, contact your next level of support or your service provider.

HSCL3xxx error codes	Message	Recovery action
HSCL3505	An error occurred while contacting the access control system. Retry the operation.	<ol style="list-style-type: none"> 1. Restart the system. 2. If the problem persists, contact your next level of support or your service provider.
HSCL350A	Invalid input parameter(s).	<ol style="list-style-type: none"> 1. Check the input and try the task again. 2. If the problem persists, contact your next level of support or your service provider.
HSCL350B	The user does not have the appropriate authority.	<ol style="list-style-type: none"> 1. Try the task again. 2. Restart the system. 3. If the problem persists, contact your next level of support or your service provider.
HSCL350C	Input error: An invalid operation has been specified.	<ol style="list-style-type: none"> 1. Check the input and try the task again. 2. Restart the system. 3. If the problem persists, contact your next level of support or your service provider.
HSCL350D	Input error: An invalid user ID has been specified.	<ol style="list-style-type: none"> 1. Check the input and try the task again. 2. If the problem persists, contact your next level of support or your service provider.
HSCL350E	Input error: An invalid task has been specified.	<ol style="list-style-type: none"> 1. Check the input and try the task again. 2. Restart the system. 3. If the problem persists, contact your next level of support or your service provider.
HSCL350F	Input error: The input resource is not valid or conflicts with the role in the operation. <ol style="list-style-type: none"> 1. Check the input and try the task again. 2. Reboot the system. 3. If the problem persists, contact your next level of support or your service provider. 	<ol style="list-style-type: none"> 1. Check the input and try the task again. 2. Restart the system. 3. If the problem persists, contact your next level of support or your service provider.
HSCL3510	Input error: An invalid role or parent role has been specified.	<ol style="list-style-type: none"> 1. Check the input and try the task again. 2. If the problem persists, contact your next level of support or your service
HSCL3511	Input error: An invalid subsystem has been specified.	<ol style="list-style-type: none"> 1. Check the input and try the task again. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3512	Input error: An invalid option has been specified.	<ol style="list-style-type: none"> 1. Check the input and try the task again. 2. If the problem persists, contact your next level of support or your service provider.
HSCL3513	Input error: An invalid managed resource role name has been specified.	<ol style="list-style-type: none"> 1. Check the input and try the task again. 2. Restart the HMC. 3. If the problem persists, contact your next level of support or your service provider.
HSCL3514	The role specified already exists.	A duplicate role name has been specified in the operation. Select a different name.

HSCL3xxx error codes	Message	Recovery action
HSCL3532	An unknown error, such as an exception, has occurred during the operation.	<ol style="list-style-type: none"> 1. Try the task again. 2. Restart the HMC. 3. If the problem persists, contact your next level of support or your service provider.
HSCL3533	Invalid operation. The input role is a system predefined role.	The operation is not allowed.
HSCL3534	An invalid assignment has been specified. The resource type of the assignment is invalid or conflicts with the user's role.	The resource type specified in the assignment is not valid or conflicts with the user role. Give the user a different assignment or role and retry the operation.
HSCL3563	The function specified is not available in the current release.	

HSCL70xx error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCL70xx error codes	Message	Recovery action
HSCL7001	The partition profile named {0} was not found.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task 3. If the problem persists, contact your next level of support or your service provider.
HSCL7002	The partition named {0} was not found.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task 3. If the problem persists, contact your next level of support or your service provider.
HSCL7003	The partition with ID {0} was not found.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task 3. If the problem persists, contact your next level of support or your service provider.
HSCL7005	The partition was not found.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. Retry the task 3. If the problem persists, contact your next level of support or your service provider.
HSCL7007	The connection information in the database is corrupted. Shut down and restart the Hardware Management Console.	<ol style="list-style-type: none"> 1. Shut down and restart the HMC to rebuild the database. 2. Try the task again.

HSCL80xx error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCL80xx error codes	Message	Recovery action
HSCL8002	The managed system entered was not found. Check your entry and retry the command.	<ol style="list-style-type: none">1. Ensure the inputs are correct.2. Retry the task.3. If the problem persists, contact your next level of support or your service provider.
HSCL8005	{0} could not be deleted because it was not found in the search order. Retry the command.	<ol style="list-style-type: none">1. Retry the operation.2. If the problem persists, contact your next level of support or your service provider.
HSCL8008	An error occurred while trying to run corrective services. Check your entry and retry the command.	This is an unexpected error. Contact your next level of support or your service provider.
HSCL8009	An error occurred while attempting to remotely connect to the server. Retry the command.	<ol style="list-style-type: none">1. An unexpected error occurred while trying to change the Web Server settings.2. Retry the command.3. If the problem persists, contact your next level of support or your service provider.
HSCL800A	An error occurred while attempting to change web server settings. Retry the command.	<ol style="list-style-type: none">1. An unexpected error occurred while trying to change the Web Server settings.2. Retry the command.3. If the problem persists, contact your next level of support or your service provider.
HSCL800B	An error occurred while attempting to change user interface server settings. Retry the command.	<ol style="list-style-type: none">1. An unexpected error occurred while trying to change the Web-based System Manager settings.2. Retry the command.3. If the problem persists, contact your next level of support or your service provider.
HSCL800C	An error occurred while attempting to change syslogd settings. Retry the command.	<ol style="list-style-type: none">1. An unexpected error occurred while trying to change the syslog settings.2. Retry the command.3. If the problem persists, contact your next level of support or your service provider.
HSCL800D	Cannot specify both IP address and hostname.	A syntax error occurred. Retry the command with only one of the options (IP address or host name) specified.
HSCL800E	An I/O exception occurred reading the file named: {0}. Check the file and try again.	<ol style="list-style-type: none">1. Check the file.2. Retry the command.3. If the problem persists, contact your next level of support or your service provider.

HSCL80xx error codes	Message	Recovery action
HSCL800F	The partition profile named {0} was not found. Check your entry and retry the command.	<ol style="list-style-type: none"> 1. Check the profile name entered to ensure that it is correct and retry the command. 2. Rebuild the managed system and retry the operation. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL8010	The system profile named {0} was not found. Check your entry and retry the command.	<ol style="list-style-type: none"> 1. Ensure that the system profile entered was correct, and retry the command. 2. If this does not work, the system profile might be corrupted. Restore the profile data. For details, see Restoring profile data. 3. If problem persists, delete and re-create a new system profile. 4. If the problem persists, contact your next level of support or your service provider.
HSCL8011	The partition with ID {0} was not found. Check your entry and retry the command.	<ol style="list-style-type: none"> 1. Ensure the correct partition ID was entered and retry the command. 2. Rebuild the managed system and retry the operation. For details, see Updating managed system or frame information. 3. If the problem persists, contact your next level of support or your service provider.
HSCL8012	The partition named {0} was not found. Check your entry and retry the command.	<ol style="list-style-type: none"> 1. Ensure you specified a valid partition. 2. Retry the command. 3. Rebuild the managed system. For details, see Updating managed system or frame information. 4. If the problem persists, contact your next level of support or your service provider.
HSCL8013	The partition specified for the {0} attribute was not found. Correct the configuration data and retry the command.	<ol style="list-style-type: none"> 1. Ensure you specified a valid partition. 2. Retry the command. 3. Rebuild the managed system. For details, see Updating managed system or frame information. 4. If the problem persists, contact your next level of support or your service provider.
HSCL8016	An unknown error occurred while trying to perform this command. Retry the command. If the error persists, contact support.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.

HSCL90xx error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

HSCL90xx error codes	Message	Recovery action
HSCL9000	This operation is not allowed because Capacity on Demand is not supported on the managed system.	
HSCL9001	The operation has failed on the managed system.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL9003	The operation has failed on the managed system. Retry the operation. If the failure persists, contact your hardware service representative.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL9004	The information could not be retrieved from the managed system.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL9005	The information could not be retrieved from the managed system. contact your next level of support or your service provider.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL9006	The information could not be retrieved from the managed system. Retry the operation. If the problem persists, contact IBM support.	<ol style="list-style-type: none"> 1. Retry the operation. 2. If the problem persists, contact your next level of support or your service provider.
HSCL9007	This operation is not allowed because Capacity on Demand for processors is not supported on the managed system	
HSCL9008	This operation is not allowed because Capacity on Demand for memory is not supported on the managed system.	
HSCL9009	This operation is not allowed because Capacity Upgrade on Demand for processors is not supported on the managed system.	
HSCL900A	This operation is not allowed because Capacity Upgrade on Demand for memory is not supported on the managed system.	
HSCL900B	This operation is not allowed because On/Off Capacity on Demand for processors is not supported on the managed system.	
HSCL900C	This operation is not allowed because On/Off Capacity on Demand for memory is not supported on the managed system.	
HSCL900D	This operation is not allowed because Reserve Capacity on Demand is not supported on the managed system.	
HSCL900E	This operation is not allowed because Trial Capacity on Demand for processors is not supported on the managed system.	
HSCL900F	This operation is not allowed because Trial Capacity on Demand for memory is not supported on the managed system.	

HSCL90xx error codes	Message	Recovery action
HSCL9010	This operation is only allowed when the managed system is in the Standby or Operating state.	<ol style="list-style-type: none"> 1. Ensure that the managed system is in the Operating or Standby state, and then try the operation again. 2. If the problem persists, contact your next level of support or your service provider.
HSCL9011	This operation is not allowed because unreturned On/Off CoD processors are currently in use on the managed system. Remove the On/Off CoD processors from partitions to make them available to be reclaimed by the system, then try the operation again.	<p>Currently there are unreturned On/Off CoD processors in use on the managed system. Before this operation is allowed they must be made available to be reclaimed by the system.</p> <ol style="list-style-type: none"> 1. Check the number of unreturned On/Off CoD processors, and then remove processors from partitions, if necessary, until the number of available processors is equal to or greater than the number of On/Off CoD processors that were unreturned. 2. To remove them, either use dynamic partitioning to remove the On/Off CoD processors from a running partition, or shut down and then delete the partition to release the processors. 3. Retry the operation.
HSCL9012	This operation is not allowed because unreturned On/Off CoD memory is currently in use on the managed system. Remove the On/Off CoD memory from partitions to make it available to be reclaimed by the system, then try the operation again.	Remove the On/Off CoD memory from partitions to make it available to be reclaimed by the system, then try the operation again.
HSCL9013	This operation is not allowed because unreturned Trial CoD processors are currently in use on the managed system. Immediately remove the Trial CoD processors from partitions to make them available to be reclaimed by the system, or enter a CUoD processor activation code to permanently activate this capacity.	Immediately remove the Trial CoD processors from partitions to make them available to be reclaimed by the system, or enter a CUoD processor activation code to permanently activate this capacity.
HSCL9014	This operation is not allowed because unreturned Trial CoD memory is currently in use on the managed system. Immediately remove the Trial memory from partitions to make it available to be reclaimed by the system, or enter a CUoD memory activation code to permanently activate this capacity.	Immediately remove the Trial memory from partitions to make it available to be reclaimed by the system, or enter a CUoD memory activation code to permanently activate this capacity.
HSCL9015	The managed system cannot currently process this operation. This condition is temporary. Retry the operation.	<ol style="list-style-type: none"> 1. The managed system is busy, but the condition is temporary. Retry the operation after a period of time. 2. If the condition persists, contact your next level of support or your service provider.
HSCL9016	You did not enter the CoD code correctly. Try again.	The CoD code was entered incorrectly. Try the operation again by carefully re-entering the code exactly as it was given to you.

HSCL90xx error codes	Message	Recovery action
HSCL9017	{0} The sequence number of the CoD code indicates that this code has been used before. Obtain a new CoD code and try again.	The CoD code that was entered has been used before and cannot be used more than once. Check to make sure you are entering a new CoD code and try again.
HSCL9018	{0} The CoD feature for which the CoD code was generated is not supported on the managed system.	The CoD feature for which this CoD code was generated is not supported on the managed system. Verify that the CoD code you are trying to enter was generated for the managed system on which you are trying to enter it.
HSCL9019	The CoD code has been rejected by the managed system because too many invalid CoD codes have been entered. The managed system must be rebooted before another CoD code will be accepted.	<ol style="list-style-type: none"> 1. Restart the HMC. 2. Try the task again with a valid CoD code.
HSCL901A	{0} Not enough inactive processors are available to accept this CoD code because On/Off CoD processors are currently activated. Remove some On/Off CoD processors from partitions, if necessary, to make them available to be reclaimed by the system. Then deactivate those On/Off CoD processors to reduce the number of activated On/Off CoD processors, and enter the CUoD processor activation code again.	<p>Currently, there are not enough inactive processors available to accept this CoD code for CUoD processors, because On/Off processors are currently activated.</p> <ol style="list-style-type: none"> 1. Check the number of available processors, and then remove processors from logical partitions, if necessary, until the number of available processors is equal to or greater than the number of On/Off processors that have been activated. To do this, either use dynamic partitioning to remove the On/Off CoD processors from a running partition, or shut down and then delete the partition to release the processors. 2. If the problem persists, contact your next level of support or your service provider.
HSCL901B	{0} Not enough inactive memory is available to accept this CoD code because On/Off CoD memory is currently activated. Remove some On/Off CoD memory from partitions, if necessary, to make it available to be reclaimed by the system. Then deactivate that On/Off CoD memory to reduce the amount of activated On/Off CoD memory, and enter the CUoD memory activation code again.	<p>There is not enough inactive memory currently available to accept this CUoD memory activation code, because On/Off CoD memory is currently activated.</p> <ol style="list-style-type: none"> 1. Check the amount of available system memory, and then remove memory from partitions, if necessary, until the amount of available system memory is equal to or greater than the amount of On/Off CoD memory that has been activated. (Use dynamic partitioning to remove memory from one or more running partitions, or delete one or more shut down partitions to release memory.) 2. Deactivate the On/Off CoD memory. 3. Retry the operation.
HSCL901C	{0} There are not enough inactive processors available to accept this CoD code because Trial CoD processors are currently activated. Either wait until the current Trial CoD activation period expires, or stop the current trial. Then enter the CUoD processor activation code again.	<ol style="list-style-type: none"> 1. Wait until the current Trial CoD activation period expires, or stop the current trial. 2. Retry the operation.

HSCL90xx error codes	Message	Recovery action
HSCL901D	{0} There is not enough inactive memory available to accept this CoD code because Trial CoD memory is currently activated. Either wait until the current Trial CoD activation period expires, or stop the current trial. Then enter the CUoD memory activation code again.	<ol style="list-style-type: none"> 1. Wait until the current Trial CoD activation period expires, or stop the current trial. 2. Retry the operation.
HSCL901E	{0} Not enough inactive processors are available to accept this CoD code because On/Off CoD processors and Trial CoD processors are currently activated. Remove some On/Off CoD processors or Trial CoD processors from partitions, if necessary, to make them available to be reclaimed by the system. Then deactivate those On/Off CoD and/or Trial CoD processors to reduce the number of activated CoD processors, and enter the CUoD processor activation code again.	
HSCL901F	{0} Not enough inactive memory is available to accept this CoD code because On/Off CoD memory and Trial CoD memory are currently activated. Remove some On/Off CoD memory or Trial CoD memory from partitions, if necessary, to make it available to be reclaimed by the system. Then deactivate that On/Off CoD and/or Trial CoD memory to reduce the amount of activated CoD memory, and enter the CUoD memory activation code again.	
HSCL9020	{0} The CoD code cannot be accepted because Trial CoD processors are already activated on the managed system.	A Trial processor code cannot be accepted when Trial CoD processors are already activated.
HSCL9021	{0} The CoD code cannot be accepted because Trial CoD memory is already activated on the managed system.	<p>A Trial memory code cannot be accepted when Trial CoD memory is already activated.</p> <ol style="list-style-type: none"> 1. Wait until the current Trial CoD activation period expires, or stop the current Trial. 2. Retry the operation.

HSCL90xx error codes	Message	Recovery action
HSCL9022	{0} Not enough inactive processors are available to accept this CoD code because On/Off CoD processors are currently activated. Remove some On/Off CoD processors from partitions, if necessary, to make them available to be reclaimed by the system. Then deactivate those On/Off CoD processors to reduce the number of activated On/Off CoD processors, and enter the Trial processor code again.	<p>There are not enough inactive processors currently available to accept this Trial processor code, because On/Off CoD processors are currently activated.</p> <ol style="list-style-type: none"> 1. Check the number of available system processors, and then remove processors from partitions, if necessary, until the number of available system processors is equal to or greater than the number of On/Off CoD processors that have been activated. (Use dynamic partitioning to remove processors from one or more running partitions, or delete one or more shut down partitions to release the processors.) 2. Deactivate the On/Off CoD processors. 3. Retry the operation.
HSCL9023	{0} There is not enough inactive memory available to accept this CoD code because On/Off CoD memory is currently activated. If necessary, remove memory from partitions until the amount of On/Off CoD memory that is activated has been made available to be reclaimed by the system. Then deactivate the On/Off CoD memory, and reenter the Trial memory code.	<p>There is not enough inactive memory currently available to accept this Trial memory code, because On/Off CoD memory is currently activated.</p> <ol style="list-style-type: none"> 1. Check the amount of available system memory, and then remove memory from partitions, if necessary, until the amount of available system memory is equal to or greater than the amount of On/Off CoD memory that has been activated. (Use dynamic partitioning to remove memory from one or more running partitions, or delete one or more shut down partitions to release the memory.) 2. Deactivate the On/Off CoD memory. 3. Retry the operation.
HSCL9024	{0} The CoD code cannot be accepted because On/Off CoD resources are currently activated. If necessary, remove resources from partitions until the amount of On/Off CoD resources that are activated have been made available to be reclaimed by the system. Then deactivate the On/Off CoD resources, and re-enter the On/Off capacity termination code.	<p>The CoD code to terminate On/Off CoD cannot be accepted, because On/Off resources are currently activated.</p> <ol style="list-style-type: none"> 1. Check the amount of available resources, and then remove resources from partitions, if necessary, until the amount of available resources is equal to or greater than the amount of resources that have been activated for CoD. Do this by either using dynamic partitioning to remove the On/Off resources from a running partition, or shut down and delete the partition to release the resources. 2. Retry the operation.
HSCL9025	{0} The CoD code cannot be accepted because there are insufficient resources available on the managed system.	<ol style="list-style-type: none"> 1. If there are temporary CoD resources activated on your system, deactivate them. 2. Retry the operation.

HSCL90xx error codes	Message	Recovery action
HSCL9026	The number of On/Off CoD processors requested exceeds the number of inactive processors that are currently available on the managed system. Reduce the number of processors requested and try again.	<ol style="list-style-type: none"> 1. Reduce the number of processors requested. 2. Retry the operation.
HSCL9027	The amount of On/Off CoD memory requested exceeds the amount of inactive memory that is currently available on the managed system. Reduce the amount of memory requested and try again.	<ol style="list-style-type: none"> 1. Reduce the amount of memory requested so that the amount requested is less than or equal to the amount of inactive memory available for On/Off CoD. 2. Retry the operation.
HSCL9028	Not enough On/Off CoD processor days remain to accept the On/Off CoD processor activation request. Either reduce the number of processors and/or days requested or obtain and enter a new On/Off processor enablement code.	<ol style="list-style-type: none"> 1. Reduce the number of processors or days requested so that the number of processor days requested (the number of processors multiplied by the number of days) is less than or equal to the number of processor days available for new On/Off CoD requests. 2. Alternatively, obtain and enter a new On/Off processor enablement code.
HSCL9029	Not enough On/Off CoD memory days remain to accept the On/Off CoD memory activation request. Either reduce the amount of memory and/or number of days requested or obtain and enter a new On/Off memory enablement code.	<ol style="list-style-type: none"> 1. Reduce the amount of memory or number of days requested so that the number of memory days requested (the GBs of memory multiplied by the number of days) is less than or equal to the number of memory days available for new On/Off CoD requests. 2. Alternatively, obtain and enter a new On/Off memory enablement code.
HSCL902A	There are insufficient resources available to accept the On/Off CoD activation request.	<p>The number of processors multiplied by the number of days cannot exceed the number of processor days remaining in the current On/Off CoD processor enablement period.</p> <ol style="list-style-type: none"> 1. Reduce either the number of processors or the number of days by amounts such that the product of these two values is less than or equal to the number of processor days remaining in the current On/Off CoD processor enablement period. 2. Alternatively, you might obtain another On/Off CoD processor enablement code to extend your On/Off CoD processor enablement period.
HSCL902B	The On/Off CoD processor activation request cannot be accepted because On/Off CoD processors are currently activated. The Current On/Off CoD processors must be deactivated before a new On/Off CoD processor activation request can be accepted.	<p>On/Off CoD processors are already activated.</p> <ol style="list-style-type: none"> 1. Deactivate current On/Off CoD processors. 2. Retry the operation.

HSCL90xx error codes	Message	Recovery action
HSCL902C	The On/Off CoD memory activation request cannot be accepted because On/Off CoD memory is currently activated. The current On/Off CoD memory must be deactivated before a new On/Off CoD memory activation request can be accepted.	On/Off CoD memory is already activated. 1. Deactivate the current On/Off CoD memory. 2. Retry the operation
HSCL902D	The On/Off CoD processor activation request cannot be accepted because Trial CoD processors are currently activated. Either wait until the current Trial CoD activation period expires, or stop the current trial. Then retry the On/Off CoD processor activation request.	1. Wait until the current Trial CoD activation period expires, or stop the current trial. 2. Retry the operation.
HSCL902E	The On/Off CoD memory activation request cannot be accepted because Trial CoD memory is currently activated. Either wait until the current Trial CoD activation period expires, or stop the current trial. Then retry the On/Off CoD memory activation request.	1. Wait until the current Trial CoD activation period expires, or stop the current trial. 2. Retry the operation.
HSCL902F	The number of processors to activate is not valid. The number must be a multiple of {0} processors. Correct your entry, and try again.	1. Enter a valid number of processors. 2. Retry the operation.
HSCL9030	The amount of memory to activate is not valid. The amount must be a multiple of {0} GB. Correct your entry, and try again.	1. Enter a valid amount of memory. 2. Retry the operation.
HSCL9031	On/Off CoD processors are not currently enabled on the managed system. An On/Off processor enablement code must be obtained and entered before On/Off CoD processors can be activated.	On/Off CoD processors are not currently enabled on the system. Obtain an On/Off CoD processor enablement code, and then try again to activate the processors after the enablement code has been entered.
HSCL9032	On/Off CoD for memory is not currently enabled on the managed system. An On/Off memory enablement code must be obtained and entered before On/Off CoD memory can be activated.	An On/Off memory enablement code must be obtained and entered before On/Off CoD memory can be activated. 1. Obtain and enter an On/Off memory enablement code. 2. Retry the operation.
HSCL9033	The On/Off CoD processor deactivation request cannot be accepted because there are no On/Off CoD processors that are currently activated on the managed system.	An attempt was made to deactivate processors that have not been activated; therefore, there is no recovery action.
HSCL9034	The On/Off CoD memory deactivation request cannot be accepted because there is no On/Off CoD memory that is currently activated on the managed system.	

HSCL90xx error codes	Message	Recovery action
HSCL9035	The On/Off CoD processors cannot be deactivated because they cannot be reclaimed by the managed system. Remove processors from partitions to make them available to be reclaimed by the system, then try again.	<p>An attempt was made to deactivate On/Off CoD processors when there are not enough available processors for the system to reclaim.</p> <ol style="list-style-type: none"> 1. Deallocate the processors by checking the number of available processors and removing processors from partitions, if necessary, until the number available is equal to or greater than the number of processors that have been activated for On/Off CoD. Either use dynamic partitioning to remove the On/Off processors from a running partition, or shut down and delete the partition to release the processors. 2. Retry the operation.
HSCL9036	The On/Off CoD memory cannot be deactivated because it cannot be reclaimed by the managed system. Remove memory from partitions to make it available to be reclaimed by the system, then try again.	<p>An attempt was made to deactivate On/Off CoD memory when there is not enough available memory for the system to reclaim.</p> <ol style="list-style-type: none"> 1. Check the amount of available system memory, and then remove memory from partitions, if necessary, until the amount of available system memory is equal to or greater than the amount of On/Off CoD memory that is activated. (Use dynamic partitioning to remove memory from one or more running partitions, or delete one or more shut down partitions to release the memory.) 2. Retry the operation.
HSCL9037	This request cannot be accepted because a CoD processor trial is not currently running on the managed system.	
HSCL9038	This request cannot be accepted because a CoD memory trial is not currently running on the managed system.	
HSCL9039	This request cannot be accepted because the activated Trial CoD processors cannot be reclaimed by the managed system. Remove processors from partitions to make them available to be reclaimed by the system, then try again.	<p>An attempt was made to stop a CoD processor trial when there are not enough available processors for the system to reclaim.</p> <ol style="list-style-type: none"> 1. Check the number of available system processors, and then remove processors from partitions, if necessary, until the number of available system processors is equal to or greater than the number of Trial CoD processors that are activated. (Use dynamic partitioning to remove processors from one or more running partitions, or delete one or more shut down partitions to release the processors.) 2. Retry the operation.

HSCL90xx error codes	Message	Recovery action
HSCL903A	This request cannot be accepted because the activated Trial CoD memory cannot be reclaimed by the managed system. Remove memory from partitions to make it available to be reclaimed by the system, then try again.	An attempt was made to stop a CoD memory trial when there is not enough available memory for the system to reclaim. 1. Check the amount of available system memory, and then remove memory from partitions, if necessary, until the amount of available system memory is equal to or greater than the amount of Trial CoD memory that is activated. (Use dynamic partitioning to remove memory from one or more running partitions, or delete one or more shut down partitions to release the memory.) 2. Retry the operation.
HSCL903B	An error occurred while trying to save the information to a diskette. Verify that the diskette is writeable and try the operation again. If the problem persists, contact your service representative.	Verify that the diskette is writeable and try the operation again. If the problem persists, contact your service representative.
HSCL903D	The Reserve CoD processor activation request cannot be accepted because On/Off CoD processors are currently activated. Either wait until the On/Off CoD processor request expires, or cancel the current On/Off processor activation request. Then try the Reserve CoD processor activation request again.	1. Either wait until the On/Off CoD processor request expires, or cancel the current On/Off processor activation request. 2. Then retry the Reserve CoD processor activation request.
HSCL903E	The On/Off CoD processor activation request cannot be accepted because Reserve CoD processors are currently activated. The Reserve CoD processors must be deactivated before an On/Off CoD processor activation request can be accepted.	The Reserve CoD processors must be deactivated before an On/Off CoD processor activation request can be accepted.
HSCL903F	The Reserve CoD processor activation request cannot be accepted because Trial CoD processors are currently activated. Either wait until the Trial CoD activation period expires, or stop the current trial. Then try the Reserve CoD processor activation request again.	Either wait until the Trial CoD activation period expires, or stop the current trial. Then retry the Reserve CoD processor activation request.
HSCL9040	The number of CoD processors requested exceeds the number of inactive processors that are currently available on the managed system. Reduce the number of processors and try again.	Reduce the number of processors and try the operation again.
HSCL9041	Not enough processor days remain to accept the Reserve CoD processor activation request. Either reduce the number of processors requested or obtain and enter an additional Reserve capacity prepaid code.	Either reduce the number of processors requested, or obtain and enter an additional Reserve CoD processor enablement code.
HSCL9042	Reserve CoD for processors is not currently enabled on the managed system. A Reserve capacity prepaid code must be obtained and entered before Reserve CoD processors can be activated.	A Reserve processor enablement code must be obtained and entered before Reserve CoD processors can be activated. Enter a Reserve processor enablement code, and then try the operation again.

HSCL90xx error codes	Message	Recovery action
HSCL9043	The Reserve CoD deactivation request cannot be accepted because there are no Reserve CoD processors currently activated on the managed system.	Reserve CoD processors need to be activated before a deactivation request can be accepted.
HSCL9044	{0} There are not enough inactive processors available to accept this CoD code because Reserve CoD processors are currently activated. Reserve CoD processors must be deactivated before this CoD code can be accepted.	To make the processors available to be reclaimed by the system, deactivate Reserve CoD processors. Then re-enter the CUoD processor activation code.
HSCL9045	{0} There are not enough inactive processors available to accept this CoD code because Reserve CoD processors are currently activated. Reserve CoD processors must be deactivated before this CoD code can be accepted.	To make the processors available to be reclaimed by the system, deactivate the Reserve CoD processors. Then re-enter the Trial CoD processor activation code.
HSCL9046	{0} The On/Off processor enablement code cannot be accepted because Reserve CoD processors are currently activated. The Reserve CoD processors must be deactivated before an On/Off CoD processor enablement code can be accepted.	The Reserve CoD processors must be deactivated before an On/Off CoD processor enablement code can be accepted. Deactivate the Reserve CoD processors, and try the operation again.
HSCL9047	{0} The Reserve capacity prepaid code cannot be accepted because On/Off CoD processors are currently activated. The On/Off CoD processors must be deactivated before a Reserve capacity prepaid code can be accepted.	The On/Off CoD processors must be deactivated before a Reserve CoD processor enablement code can be accepted. Deactivate the On/Off CoD processors, and try the operation again.
HSCL9048	This operation is not allowed because unreturned CoD processors are currently in use on the managed system.	<ol style="list-style-type: none"> 1. Check the number of unreturned On/Off CoD or Trial CoD processors that are currently in use. Remove that number of processors from partitions. (Use dynamic partitioning to remove processors from one or more running partitions, or delete one or more shut down partitions to release the processors.) 2. Retry the operation.
HSCL9049	This operation is not allowed because unreturned CoD memory is currently in use on the managed system.	<ol style="list-style-type: none"> 1. Check the amount of unreturned On/Off CoD or Trial CoD memory that is currently in use. Remove that amount of memory from partitions. (Use dynamic partitioning to remove memory from one or more running partitions, or delete one or more shut down partitions to release the memory.) 2. Retry the operation.

HSCL90xx error codes	Message	Recovery action
HSCL904A	The activation code you entered has been rejected because it is not a Capacity on Demand code.	<p>An attempt was made to enter an activation code that is not a Capacity on Demand code. The code might be a Virtualization Engine systems technologies activation code.</p> <p>If you intended to enter a Virtualization Engine systems technologies code, then select Manage On Demand Activations > Virtualization Engine Technologies > Enter Activation Code and try again.</p> <p>If you intended to enter a Capacity on Demand activation code, then obtain a Capacity on Demand activation code for this system and try again.</p>
HSCL904B	This operation is not allowed because Mobile Capacity on Demand for processors is not supported on the managed system.	No recovery action.
HSCL904C	This operation is not allowed because Mobile Capacity on Demand for memory is not supported on the managed system.	No recovery action.
HSCL904D	The Capacity on Demand code type specified is not supported by the managed system.	No recovery action.
HSCL904E	{0} The CoD code cannot be accepted because the number of processors to be removed exceeds the number of permanent processors than can be removed on the managed system.	If possible, obtain and enter a new Mobile CoD processor remove code for removal of fewer processors.
HSCL904F	{0} The CoD code cannot be accepted because the amount of memory to be removed exceeds the amount of permanent memory than can be removed on the managed system.	If possible, obtain and enter a new Mobile CoD memory remove code for removal of less memory.
HSCL9050	{0} The CoD code cannot be accepted because the number of processors to be removed exceeds the number of processors that are currently available on the managed system.	Either remove processors from logical partitions to make them available to be removed, or if possible, obtain and enter a new Mobile CoD processor remove code for removal of fewer processors.
HSCL9051	{0} The CoD code cannot be accepted because the amount of memory to be removed exceeds the amount of memory that is currently available on the managed system.	Either remove memory from logical partitions to make it available to be removed, or if possible, obtain and enter a new Mobile CoD memory code for removal of less memory.
HSCL9052	The additional number of On/Off CoD processors requested exceeds the number of inactive processors that are currently available on the managed system. Reduce the number of processors requested and try again.	Reduce the number of processors requested and try again.
HSCL9053	The additional amount of On/Off CoD memory requested exceeds the amount of inactive memory that is currently available on the managed system. Reduce the amount of memory requested and try again.	Reduce the amount of memory requested and try again.

HSCL90xx error codes	Message	Recovery action
HSCL9054	The request to reduce the number of On/Off CoD processors cannot be accepted. The On/Off CoD processors to be deactivated cannot be deactivated because they cannot be reclaimed by the managed system. Remove processors from partitions to make them available to be reclaimed, then try again.	Remove processors from partitions to make them available to be reclaimed, then try again.
HSCL9055	The number of days specified is not valid.	No recovery action.
HSCL9056	The number of days specified is not valid.	No recovery action.

HSCLAxxx error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

[Back to HSCL error codes page](#)

HSCLAxxx error codes	Message	Recovery action
HSCLA000	This operation is not allowed because activation of Virtualization Engine Technologies are not supported on the managed system.	Virtualization Engine Technologies activations are not supported on the managed system. If this is incorrect, contact your software representative.
HSCLA001	The Show Code Information operation failed. Try the operation again.	Try the operation again. If the problem persists, contact your software representative.
HSCLA002	The Enter Activation Code operation failed. Try the operation again.	Try the operation again. If the problem persists, contact your software representative.
HSCLA003	You did not enter the activation code correctly. Try again.	Enter the activation code again, ensuring that it is correct. If you are certain that you entered the correct activation code, contact your Virtualization Engine systems technologies administrator.
HSCLA004	{0} The sequence number of the activation code indicates that this code has been used before. Obtain a new activation code and try again.	Obtain a new activation code and try the operation again. If the problem persists, contact your Virtualization Engine systems technologies administrator.
HSCLA005	{0} The capability for which the activation code was generated is not supported on the managed system.	The activation code that was entered is for a capability that is not supported on the managed system. <ol style="list-style-type: none"> 1. Obtain a new activation code and try the operation again. 2. If the problem persists, contact your Virtualization Engine systems technologies administrator.
HSCLA006	[0] The operation failed on the managed system. Try the operation again. If the failure persists, contact your hardware service representative.	Try the operation again. If the failure persists, contact your next level of support or your hardware service provider.

HSCLA_{xxx} error codes	Message	Recovery action
HSCLA007	{0} The activation code was rejected by the managed system because too many incorrect activation codes have been entered. The managed system must be restarted before another activation code will be accepted.	Restart the managed system, and retry the operation.
HSCLA008	The activation code entered is a CoD activation code instead of a Virtualization Engine Technologies activation code. Try again.	<ol style="list-style-type: none"> 1. Make sure to obtain a Virtualization Engine Technologies activation code for this system. 2. Try the operation again. 3. If the problem persists, contact your Virtualization Engine systems technologies administrator.
HSCLA009	The activation code was rejected by the managed system because it is not valid. Contact your Virtualization Engine Technologies administrator.	If the problem persists, contact your Virtualization Engine systems technologies administrator.
HSCLA00A	The activation code is the wrong length. The code entered must be exactly {0} characters long. Try again.	<ol style="list-style-type: none"> 1. Make sure that your activation code is correct, and is exactly 34 characters in length. 2. Try the operation again. 3. If the problem persists, contact your Virtualization Engine systems technologies administrator.
HSCLA00B	Unknown code information format. Try the operation again.	Try the operation again. You might need to upgrade to a newer HMC level to fix this problem. If the problem persists, contact your service provider.
HSCLA101	The bulk power assembly that was specified is not valid. Verify the bulk power assembly target name and try the request again.	<ol style="list-style-type: none"> 1. Rebuild the managed frame. For details, see Updating managed system or frame information. 2. Try the task again. 3. If the problem persists, contact your service provider.
HSCLA110	The managed system does not support service processor failover.	No recovery action.

HSCLP_{xxxx} platform management error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

HSCLP_{xxxx} error codes	Message	Recovery action
HSCLP0001	The Backup Critical Data request completed successfully.	
HSCLP0002	Ensure the media is inserted correctly into the drive and try the operation again.	Verify that the media is inserted correctly in the drive and try the operation again.
HSCLP0003	The Backup Critical Data request failed.	An internal HMC error occurred. Contact your next level of support or your service provider.

HSCP _{xxxx} error codes	Message	Recovery action
HSCP0004	The media is write protected. Remove write protection and try the operation again.	Remove write protection and try the operation again.
HSCP0005	The Backup Critical Data request is in progress. Please wait.	
HSCP0010	The Format Removable Media request completed successfully.	
HSCP0011	Ensure the media is inserted correctly into the drive and try the operation again.	
HSCP0012	The media is write protected. Remove the write protection and try the operation again.	
HSCP0013	An unknown error occurred. Replace the media and try the operation again.	
HSCP0014	The Format Removable Media request failed.	
HSCP0015	Please wait while the media is being formatted.	
HSCP0020	The Save Upgrade Data request completed successfully.	
HSCP0021	The Save Upgrade Data request failed.	
HSCP0022	The Save Upgrade Data request failed. Ensure the removable media is inserted correctly into the drive.	
HSCP0023	The media is write protected. Remove the write protection and try the operation again.	
HSCP0024	An error occurred while copying the upgrade data. Ensure the removable media is inserted correctly into the drive and retry the operation.	
HSCP0025	An error occurred while saving the upgrade data. Try the operation again. If the problem continues, contact your service representative.	
HSCP0026	An error occurred while trying to mount the media. Ensure the removable media is inserted correctly and try the operation again.	
HSCP0027	An error occurred while trying to unmount the media. Ensure the media is not being shared.	
HSCP0028	An non-recoverable error occurred. Refer to the HMC console log for detailed information.	<ol style="list-style-type: none"> 1. Refer to the HMC console log for more information. 2. If the problem persists, contact your next level of support or your service provider.
HSCP0029	An error occurred while instantiating the save upgrade data target class.	
HSCP0030	An error occurred creating the file that processes the save upgrade data on the next reboot. Try the operation again.	<ol style="list-style-type: none"> 1. Rebuild the managed system. For details, see Updating managed system or frame information. 2. If the problem persists, contact your next level of support or your service provider.

HSCPxxxx error codes	Message	Recovery action
HSCP0031	Generating archives of subsystem files. Please wait.	
HSCP0040	The corrective service file was successfully downloaded to this system console. Press OK to continue and install this update.	
HSCP0041	The corrective service file was successfully applied. Wait until all tasks complete and reboot the HMC for the changes to take place.	
HSCP0042	An unrecoverable error occurred during the corrective service file download. Try the operation again. If the problem continues, contact your service representative.	<ol style="list-style-type: none"> 1. Try the task again. 2. If the problem persists, contact your next level of support or your service provider.
HSCP0043	An unrecoverable error occurred during the corrective service installation. Try the operation again. If the problem continues, contact your service representative.	<ol style="list-style-type: none"> 1. Try the operation again. 2. If the problem persists, contact your next level of support or your service provider.
HSCP0044	The removable media cannot be mounted. Ensure the media is inserted correctly into the drive and try the operation again.	<ol style="list-style-type: none"> 1. Verify that the removable media is correctly inserted in the drive and try the operation again. 2. If the error persists, contact your next level of support or your service provider.
HSCP0045	The corrective service data is corrupt. Ensure the media is inserted correctly into the drive and try the operation again.	<ol style="list-style-type: none"> 1. Verify that the removable media is correctly inserted in the drive and try the operation again. 2. If the error persists, contact your next level of support or your service provider.
HSCP0046	An error occurred while attempting to remotely connect to the server. Try the operation again. If the problem continues, contact your service representative.	<ol style="list-style-type: none"> 1. Try the operation again. 2. If the problem persists, contact your next level of support or your service provider.
HSCP0047	An unspecified error occurred while downloading the corrective service file. Try the operation again. If the problem continues, contact your service representative.	<ol style="list-style-type: none"> 1. Try the operation again. 2. If the problem persists, contact your next level of support or your service provider.
HSCP0048	An unknown error occurred. Try the operation again. If the problem continues, contact your service representative.	<ol style="list-style-type: none"> 1. Try the task again. 2. If the problem persists, contact your next level of support or your service provider.
HSCP0049	The Install Corrective Service request is in progress. Please wait.	
HSCP0050	The download file is corrupt. Try the operation again.	
HSCP0051	The corrective service file download was unsuccessful.	Refer to the text on the error message window.
HSCP0052	Successfully downloaded file. Installing, please wait.	
HSCP0053	Corrective service installation was successful.	

HSCP _{xxxx} error codes	Message	Recovery action
HSCP0054	Corrective service installation has failed.	Refer to the text on the error message window.
HSCP0055	View the console log for details.	
HSCP0056	Halting service installation.	
HSCP0057	Corrective service file download in progress...	
HSCP0058	The corrective service file downloaded successfully, continuing...	
HSCP0060	The Customize Date/Time request completed successfully. Please reboot the HMC.	1. Shut down and restart the HMC. For details, see Shutting down, rebooting, and logging off the HMC.
HSCP0061	The Customize Date/Time request failed.	<ol style="list-style-type: none"> 1. Verify that the removable media is correctly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the problem persists, contact your next level of support or your service provider.
HSCP0070	Enter an integer value between 1 and 99.	
HSCP0071	You cannot schedule an event in the past. Set the date and time to schedule the event in the future.	Select a date and time that is after the present time.
HSCP0080	There are no system events.	
HSCP0081	Unable to display the log data.	<ol style="list-style-type: none"> 1. Verify that the removable media is correctly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the problem persists, contact your next level of support or your service provider.
HSCP0082	Unable to retrieve log data.	<ol style="list-style-type: none"> 1. Verify that the removable media is correctly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the problem persists, contact your next level of support or your service provider.
HSCP0083	An error occurred while processing the exit request.	<ol style="list-style-type: none"> 1. Verify that the removable media is correctly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the problem persists, contact your next level of support or your service provider.

HSCP _{xxxx} error codes	Message	Recovery action
HSCP0090	Cannot check both the 'Export default gateway' and 'Silent' options for 'routed'.	Select either Export default gateway or Silent for the Routed option.
HSCP0091	Your updates have been saved to the system configuration files. You may need to reboot for all Network Settings changes to take affect.	Restart the HMC.
HSCP0092	Unable to save your Network Settings updates to the system configuration files.	<ol style="list-style-type: none"> 1. Try the operation again. 2. Shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.
HSCP0093	Ethernet driver {1} cannot be set to {0}.	<ol style="list-style-type: none"> 1. Select a valid speed for the adapter. 2. Select Auto-negotiate speed. 3. Shut down and restart the HMC.
HSCP0100	No managed systems were detected that are attached to this system console.	<ol style="list-style-type: none"> 1. If you have a managed system attached, shut down and restart the HMC. 2. If the problem persists, contact your next level of support or your service provider.
HSCP0101	No logical partitions have been defined for this managed system.	<ol style="list-style-type: none"> 1. Check to ensure that Service Focal Point is communicating correctly with the managed system. 2. Shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.
HSCP0102	A blank or incorrect entry was entered in the partition password field.	Re-enter a valid password in the entry field and try the operation again.
HSCP0103	A blank or incorrect entry was entered in the listening port field.	Re-enter a valid listening port and try the operation again.
HSCP0104	A blank or incorrect entry was entered in the IP address field.	Re-enter the IP address and try the operation again.
HSCP0110	The Inventory Scout Services command completed successfully.	
HSCP0111	The Inventory Scout Services command request failed.	<ol style="list-style-type: none"> 1. Try the operation again. 2. Shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.
HSCP0112	The removable media cannot be mounted. Ensure the media is inserted correctly into the drive and try the operation again.	<ol style="list-style-type: none"> 1. Insert a correctly formatted diskette into the drive. 2. Try using an alternate diskette. 3. If the error persists, contact your next level of support or your service provider.
HSCP0113	The media is write protected. Remove the write protection and try the operation again.	Remove write protection on the media and retry the operation.

HSCP _{xxxx} error codes	Message	Recovery action
HSCP0114	The Inventory Scout request failed. Ensure the removable media is inserted correctly into the drive.	<ol style="list-style-type: none"> 1. Insert the correctly formatted diskette into the drive. 2. Try using an alternate diskette. 3. If the error persists, contact your next level of support or your service provider.
HSCP0115	An error occurred while copying the Inventory Scout data. Verify that a blank formatted diskette is inserted correctly in the drive and retry the operation.	<ol style="list-style-type: none"> 1. Ensure that there is enough space on the media. 2. Try using an alternate diskette and retry the operation. 3. If the error persists, contact your next level of support or your service provider.
HSCP0116	An error occurred while compressing the Inventory Scout data. Try the operation again.	
HSCP0117	An error occurred while trying to unmount the media.	
HSCP0118	The Inventory Scout daemon was restarted successfully.	
HSCP0119	The Inventory Scout daemon cannot be restarted. Reboot the HMC and try the operation again.	<ol style="list-style-type: none"> 1. Try the operation again. 2. Shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.
HSCP0120	The CEC name is malformed.	<ol style="list-style-type: none"> 1. Shut down and restart the HMC. 2. If the error persists, contact your next level of support or your service provider.
HSCP0121	The Inventory Scout request failed. An error occurred while copying data to removable media.	<ol style="list-style-type: none"> 1. Retry the operation. 2. Restart the invscout daemon. 3. If the error persists, contact your next level of support or your service provider.
HSCP0122	The system partition(s) did not respond to query attempts.	<ol style="list-style-type: none"> 1. Check to ensure that Service Focal Point is communicating correctly with the managed system. 2. Shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.
HSCP0123	Unable to start the terminal session using available error data. Return to Service Management interface and attempt to start the TTY session from there.	<ol style="list-style-type: none"> 1. Return to the Service Management interface and attempt to start the virtual terminal session. 2. If the problem persists, contact your next level of support or your service provider.
HSCP0124	Unrecoverable error attempting to start a TTY session. Return to Service Management interface and attempt to start the TTY session from there.	<ol style="list-style-type: none"> 1. Return to the Service Management interface and attempt to start the virtual terminal session. 2. If the problem persists, contact your next level of support or your service provider.

HSCP _{xxxx} error codes	Message	Recovery action
HSCP0125	An incorrect user ID and password combination was entered. Specify a valid user ID and password and try the operation again.	<ol style="list-style-type: none"> 1. Specify a valid user ID and password and retry the operation. 2. Ensure that the remote service (FTP) site is operational. 3. If the problem persists, contact your next level of support or your service provider.
HSCP0126	The corrective service file was not found on the server. Ensure the correct fully qualified path and filename has been specified for the 'Patch file' field and retry the operation.	<ol style="list-style-type: none"> 1. Specify a valid user ID and password and retry the operation. 2. Ensure that the remote service (FTP) site is operational. 3. If the problem persists, contact your next level of support or your service provider.
HSCP0127	An error occurred while unpacking the corrective service file. The file may be corrupt, or the HMC may have run out of disk space. Try the operation again. If the problem continues, contact your service representative.	<ol style="list-style-type: none"> 1. Shut down and restart the HMC. 2. If the error persists, contact your next level of support or your service provider.
HSCP0128	A required file is missing from the service package. Contact your service representative.	Contact your next level of support or your service provider.
HSCP0129	An attempt was made to apply incorrect service to this version of HMC software. Ensure the correct service filename has been specified and retry the operation.	<ol style="list-style-type: none"> 1. Ensure that the correct service file name has been entered and try the operation again. 2. If the problem persists, contact your next level of support or your service provider.
HSCP0130	The target directory for service file extraction does not exist. Contact your service representative.	<ol style="list-style-type: none"> 1. Shut down and restart the HMC. 2. If the error persists, contact your next level of support or your service provider.
HSCP0131	A fatal error occurred during service file installation. The system may be unstable. Contact your service representative.	<ol style="list-style-type: none"> 1. Shut down and restart the HMC. 2. If the error persists, contact your next level of support or your service provider.
HSCP0135	Error {0} processing data on removable media.	<ol style="list-style-type: none"> 1. Attempt to download and apply the service file again. 2. Save HMC upgrade data to preserve configuration data. For details, see Saving HMC upgrade data. 3. Reinstall the HMC from the recovery CD as if doing an upgrade. 4. If the problem persists, contact your next level of support or your service provider.
HSCP0136	The corrective service file was successfully copied to the HMC. Select the Frame 'Install Corrective Service' task to apply this update.	Select the frame Install Corrective Service task to apply this update.
HSCP0137	The corrective service file was successfully downloaded to the HMC. Select the Frame 'Install Corrective Service' task to apply this update.	Select the Frame Install Corrective Service task to apply this update.

HSCPxxxx error codes	Message	Recovery action
HSCP0138	An internal error occurred during Save Upgrade Data processing. Refer to the HMC console log for detailed information and recovery actions.	Refer to the HMC console log for detailed information and recovery actions.
HSCP0139	The DVD device is currently in use. Wait until all current DVD operations have been completed and try the operation again.	
HSCP0140	The DVD media is write protected. Remove the write protection and try the operation again.	
HSCP0141	Ensure the DVD media is inserted correctly into the drive and try the operation again.	
HSCP0142	An invalid or missing file system exists on the DVD media. Reformat the DVD and try the operation again.	
HSCP0143	The DVD device is not functioning correctly. Contact your service representative.	
HSCP0144	An error was detected while mounting the remote server. Verify that the parameters have been entered correctly and try the operation again.	
HSCP0145	The userId and password combination to log in to the remote server is incorrect. Ensure the combination is valid and try the operation again.	
HSCP0146	The temporary space used to create the backup archive has been exhausted. You can attempt to free disk space by deleting any pending dump files, or contact your service representative.	
HSCP0147	An error occurred while writing the informative description for this dump file. The backup task will now continue without this information.	
HSCP0148	No dump files exist on the remote server.	
HSCP0149	No detailed dump information exists for this archive.	
HSCP0150	An error occurred while reading the backup archive detailed information. The remote server may be busy. Try the operation again.	
HSCP0151	An error occurred while downloading the archive to this HMC. View the console log to see the detailed error information. Try the operation again.	
HSCP0152	An error occurred while copying the archive to this HMC. View the console log to see the detailed error information. Try the operation again.	
HSCP0153	The Backup Critical Console Data task was completed successfully.	

HSCP_{xxxx} error codes	Message	Recovery action
HSCP0154	The critical console data archive file was successfully offloaded to this HMC. Reboot the HMC and this data will be restored.	
HSCP0155	The task is unavailable. Please try again later.	
HSCP0156	An error occurred attempting to contact the remote system. Ensure a valid hostname or IP address has been entered and try the operation again.	
HSCP0157	An unrecoverable error occurred while transferring the file to the remote server. Verify that the target environment on the remote server can accommodate the request and try the operation again. If the failure persists, initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. This will require 'hsce' authority.	
HSCP0158	VPD collection was not successful. Verify all partition profiles associated with the managed system are active and accessible. Error details:	
HSCP0159	VPD collection from the managed system was successful.	
HSCP0160	VPD collection has failed. Verify all partition profiles associated with the managed system are active and accessible. Try the operation again. Error details:	

HSCS_{xxxx} Service Focal Point error codes

These error codes can be displayed in a window that is displayed on the HMC screen during system configuration and operations.

HSCS_{xxxx} error codes	Message	Recovery action
HSCS0001	Unable to obtain Serviceable Events from the Problem Manager.	<ol style="list-style-type: none"> 1. The HMC could not retrieve the Serviceable Events. Wait and try the previous function again. 2. If the error continues, shut down and restart the HMC. 3. If error persists, contact your next level of support or your service provider.
HSCS0002	Unable to process request.	<ol style="list-style-type: none"> 1. The HMC could not process your request to make changes to the Serviceable Event. Wait and try the previous function again. 2. If the error continues, shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.

HSCSxxxx error codes	Message	Recovery action
HSCS0003	Unable to update the attribute on the Serviceable Event.	<ol style="list-style-type: none"> 1. The HMC could not process your request to make changes to the Serviceable Event. Wait and try the previous function again. 2. If the error continues, shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.
HSCS0004	At least one Serviceable Event you attempted to act on could not be located. It may have expired from the Problem Manager. Please do a new query to refresh the list of Serviceable Events and try your action again.	<ol style="list-style-type: none"> 1. The HMC could not locate the Serviceable Event you are trying to view or update. It might have expired or otherwise been closed. 2. Exit the Select Serviceable Event dialog and retry.
HSCS0005	Function Failed: Error occurred attempting to display a Serviceable Event panel.	<p>The HMC was unable to locate or launch a panel you have requested. This is an internal HMC error.</p> <ol style="list-style-type: none"> 1. Back up critical HMC data. For details, see Backing up critical HMC data. 2. If the problem persists, contact your next level of support or your service provider.
HSCS0006	This Serviceable Event might contain more information than this version of the HMC can display. You might want to upgrade your HMC to the latest version.	In order to see Serviceable Event data made available in more recent HMC versions, upgrade this HMC to the most recent version or switch to an HMC that has already been upgraded.
HSCS0008	Function Failed: An error occurred when retrieving machine names.	<ol style="list-style-type: none"> 1. Not all functions might be operating. Wait and try the previous function again. 2. If the error continues, shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.
HSCS0020	Function Failed: An error occurred when launching the Service Focal Point Settings panel.	<ol style="list-style-type: none"> 1. Not all functions might be operating. Wait and try the previous function again. 2. If the error continues, shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.
HSCS0021	Function Failed: Error occurred getting information to display the Service Focal Point settings.	<ol style="list-style-type: none"> 1. Not all functions might be operating. Wait and try the previous function again. 2. If the error continues, shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.
HSCS0022	Function Failed: An error occurred when updating Service Focal Point settings.	<ol style="list-style-type: none"> 1. Not all functions might be operating. Wait and try the previous function again. 2. If the error continues, shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.

HSCSxxx error codes	Message	Recovery action
HSCS0023	Function Failed: Error occurred processing button for the Service Focal Point Settings panel.	<ol style="list-style-type: none"> 1. Not all functions might be operating. Wait and try the previous function again. 2. If the error continues, shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.
HSCS0025	Function Failed: Error occurred while processing Double Click for the Service Focal Point Settings panel.	<ol style="list-style-type: none"> 1. Not all functions might be operating. Wait and try the previous function again. 2. If the error continues, shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.
HSCS0026	Service Focal Point settings have been saved successfully.	
HSCS0047	Function Failed: An error occurred when attempting to Close the Serviceable Event.	<ol style="list-style-type: none"> 1. Not all functions might be operating. Wait and try the previous function again. 2. If the error continues, shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.
HSCS0060	Cannot change state from Unknown for machine	The requested machine state is not allowed at this time. Close and then restart the enable and disable windows for updated machine information.
HSCS0061	Insert scratch diskette number {0} of {1}.	Insert a scratch diskette and select the appropriate button.
HSCS0062	Insert DVD cartridge and press the {0} button.	Insert a formatted DVD cartridge and push the appropriate button.
HSCS0064	No extended error data available.	Select a serviceable event that has extended error data associated with it.
HSCS0065	Error writing to floppy diskette: {0}	Ensure there is a diskette in the diskette drive. Try the operation again.
HSCS0066	Error writing to DVD cartridge: {0}	Ensure there is a formatted DVD cartridge in the DVD drive. Try the operation again.
HSCS0067	Error reading extended error data: {0}	<ol style="list-style-type: none"> 1. Not all functions might be operating. Wait and try the previous function again. 2. If the error continues, shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.
HSCS0068	Error creating temporary file: {0}	<ol style="list-style-type: none"> 1. Verify that the removable media is correctly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the problem persists, contact your next level of support or your service provider.

HSCSxxx error codes	Message	Recovery action
HSCS0069	Error writing to temporary file: {0}	<ol style="list-style-type: none"> 1. Verify that the removable media is correctly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the problem persists, contact your next level of support or your service provider.
HSCS0070	Error formatting floppy diskette: {0}	Ensure there is a diskette in the diskette drive. Try the operation again.
HSCS0071	Extended error data has been saved successfully.	
HSCS0072	The saving of extended error data has been cancelled.	No action is needed. The operation was cancelled as a result of your request.
HSCS0080	Error encountered while getting the partition information.	<ol style="list-style-type: none"> 1. Not all functions might be operating. Wait and try the previous function again. 2. If the error continues, shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.
HSCS0081	Error encountered while reading the partition information.	<ol style="list-style-type: none"> 1. Not all functions might be operating. Wait and try the previous function again. 2. If the error continues, shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.
HSCS0082	Error encountered while getting the extended error data.	<ol style="list-style-type: none"> 1. Not all functions might be operating. Wait and try the previous function again. 2. If the error continues, shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.
HSCS0083	Unexpected error encountered while saving the extended error data.	<ol style="list-style-type: none"> 1. Verify that the removable media is correctly inserted in the drive and try the operation again. 2. Try the operation with different media. 3. Run PC Doctor to determine if there is a problem with the hardware. 4. If the problem persists, contact your next level of support or your service provider.
HSCS0084	Error encountered while attempting to call home with the extended error information.	<ol style="list-style-type: none"> 1. Not all functions might be operating. Wait and try the previous function again. 2. If the error continues, shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.

HSCSxxx error codes	Message	Recovery action
HSCS0085	Error encountered while attempting to call home with the extended error information. The callsa program returned a value of {0}.	<ol style="list-style-type: none"> 1. Not all functions might be operating. Wait and try the previous function again. 2. If the error continues, shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.
HSCS0086	Request to call home the extended error information has been successfully submitted.	The operation was successful.
HSCS0087	Error encountered while attempting to call home the Serviceable Event.	<ol style="list-style-type: none"> 1. Not all functions might be operating. Wait and try the previous function again. 2. If the error continues, shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.
HSCS0088	Error encountered while attempting to call home the Serviceable Event. The callsa program returned a value of {0}.	<ol style="list-style-type: none"> 1. Not all functions might be operating. Wait and try the previous function again. 2. If the error continues, shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.
HSCS0089	Request to call home the Serviceable Event has been successfully submitted.	The operation was successful.
HSCS0090	Unexpected return code encountered while creating a temporary packaging file: {0}	<ol style="list-style-type: none"> 1. Not all functions might be operating. Wait and try the previous function again. 2. If the error continues, shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.
HSCS0096	No items selected when button was pressed.	<ol style="list-style-type: none"> 1. Not all functions might be operating. Wait and try the previous function again. 2. If the error continues, shut down and restart the HMC. 3. If the error persists, contact your next level of support or your service provider.
HSCS0100	Please wait while the extended error data is being saved.	The extended error data is being saved to the appropriate removable media.
HSCS0101	Error writing to DVD cartridge.	Ensure there is a formatted DVD cartridge in the DVD drive. Try the operation again.
HSCS0102	Error unmounting DVD cartridge after writing data successfully.	Ensure that there is a formatted DVD cartridge in the DVD drive. Try the operation again.
HSCS0103	DVD drive is already mounted.	

HSCSxxx error codes	Message	Recovery action
HSCS0104	The LED request did not complete successfully. Initiate the 'View Problems Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	Note: If you do not have 'hscpe' authority, you will not see the View Problem Logs selection in the Service Utilities menu. <ol style="list-style-type: none"> 1. Retry the task. 2. Log out and then back in to the HMC interface. 3. Shut down and restart the HMC. 4. If the problem persists, contact your next level of support or your service provider.
HSCS0105	The LED request completed successfully.	
HSCS0107	Error establishing RMC session {0}.	
HSCS0108	I/O error while creating a connection monitoring type serviceable event.	
HSCS0109	Communications to the SFP component on partition {0} are unavailable.	
HSCS0110	Error adding managed object to connection monitoring type serviceable event.	
HSCS0111	Error getting managed objects in connection monitoring type serviceable event.	
HSCS0112	Error incrementing duplicate count in connection monitoring type serviceable event.	
HSCS0113	Error getting connection monitoring type serviceable events.	
HSCS0114	Communications to the SFP component on partition {0} are unavailable. This is probably due to authentication problems.	
HSCS0115	Communications to the SFP component on partition {0} are unavailable. This is probably due to the RMC daemon on the HMC being down.	
HSCS0116	Communications to the SFP component on partition {0} are unavailable. However a network path to the partition is available.	
HSCS0117	Communications to the SFP component on partition {0} are unavailable. This is probably due to the partition being down.	
HSCS0118	Communications to the SFP component on partition {0} are unavailable. This is probably due to no network path being available.	
HSCS0119	Communications to the SFP component on partition {0} are unavailable. The return code on the call to start an RMC session was {1}.	
HSCS0120	Communications to the SFP component on partition {0} are unavailable. The return code for the session interruption was {1}.	
HSCS0121	Communications to the SFP component on partition {0} are unavailable due to no network path being available.	

HSCSxxx error codes	Message	Recovery action
HSCS0125	I/O error while creating a customer upgrade on demand type serviceable event.	
HSCS0126	An error occurred while attempting to connect to the HMC information manager. The LED command has failed. Initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	
HSCS0127	An unexpected internal error has occurred. The LED command has failed. Initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	
HSCS0128	An error occurred when attempting to query the HMC's hostname. The LED processing cannot continue.	
HSCS0129	An internal LED command processing error has occurred. The LED command has failed. Initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	
HSCS0130	The dump requested was successfully initiated. The resulting dump will automatically be offloaded to the HMC. The amount of time required for the offload will vary based on the system configuration. To view this dump, refresh the main screen accordingly.	
HSCS0131	An error occurred while attempting to connect to the HMC information manager. The dump command has failed. Initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	
HSCS0132	An unexpected internal error has occurred. The dump command has failed. Initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required. Contact your service representative.	
HSCS0133	An error occurred when attempting to query the HMC's hostname. The specified dump task cannot continue.	
HSCS0134	An internal dump command processing error has occurred. The dump command has failed. Initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	
HSCS0135	The dump offload request was successful.	
HSCS0136	The DVD device could not be locked for writing. Try the operation again.	

HSCSxxx error codes	Message	Recovery action
HSCS0137	The DVD device is write protected. Remove the write protection and try the operation again.	
HSCS0138	No DVD media was found. Insert a properly formatted DVD and try the operation again.	
HSCS0139	The DVD device returned an error. Try the operation again.	
HSCS0140	An unknown error occurred while accessing the DVD device. Try the operation again.	
HSCS0141	An error occurred while copying the selected file to the DVD media. Ensure there is available space on the media and try the operation again.	
HSCS0142	A file system error has occurred on the DVD media. Try the operation again with a properly formatted DVD.	
HSCS0143	The selected file was successfully copied to the DVD media.	
HSCS0144	The selected dump file was successfully deleted from the HMC.	
HSCS0145	An error occurred while removing the dump file from the HMC. Refresh the Manage Dumps interface table to ensure the dump file still exists on the HMC and try the operation again.	
HSCS0146	An unexpected error occurred while removing the dump file from the HMC. Initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	
HSCS0149	Error retrieving connection monitoring settings: {0}.	
HSCS0150	Error applying connection monitoring settings: {0}.	
HSCS0151	Connection monitoring settings were saved.	
HSCS0164	Your request was processed successfully.	
HSCS0170	Request to call home has been successfully submitted.	
HSCS0171	Error encountered while attempting to call home.	
HSCS0180	The ASM menu was launched successfully.	
HSCS0181	An error occurred while attempting to launch the ASM menu. Try the operation again. If the failure persists, initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required. Contact your service representative.	
HSCS0182	The Lamp Test command was successfully initiated.	

HSCSxxx error codes	Message	Recovery action
HSCS0183	An error occurred while attempting to initiate the LED Lamp Test. Try the operation again. If the failure persists, initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required. Contact your service representative.	
HSCS0184	The I/O unit ownership was successfully removed.	
HSCS0185	An error occurred while removing the I/O unit ownership. Try the operation again. If the failure persists, initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	
HSCS0186	An error occurred when attempting to invoke the Repair/Verify subsystem. Contact your service representative.	
HSCS0187	An error occurred while retrieving the current list of problems for this system. Try the operation again.	
HSCS0200	The MTMS update was successful.	
HSCS0201	The following error occurred while editing the MTMS:	
HSCS0202	The format of the MTMS is not correct.	
HSCS0203	The format of the Config ID is not correct.	
HSCS0204	The Config ID update was successful.	
HSCS0205	The following error occurred while editing the Config ID:	
HSCS0206	View the system event log file for detailed error information.	
HSCS0210	The FRU was successfully replaced.	
HSCS0211	An error occurred while replacing the FRU. Try the operation again. If the failure persists, initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	
HSCS0220	The enclosure was successfully replaced.	
HSCS0221	An error occurred while replacing the enclosure. Try the operation again. If the failure persists, initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	
HSCS0222	The LED deactivation command completed successfully. Note: There still may be open problems within the system and the System Attention LED cannot be manually activated.	

HSCSxxx error codes	Message	Recovery action
HSCS0223	The LED deactivation command completed successfully. Note: There still may be open problems within the logical partition and the System Attention LED cannot be manually activated.	
HSCS0224	An error encountered while attempting to call home the selected dump. Try the operation again. If the failure persists, initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	
HSCS0225	The request to call home the selected dump has been successfully submitted.	
HSCS0226	The selected dump file size is too large to be called home. Offload the dump to DVD media and contact your service representative.	
HSCS0227	The FRU was successfully removed.	
HSCS0228	An error occurred while removing the FRU. Try the operation again. If the failure persists, initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	
HSCS0229	The enclosure was successfully removed.	
HSCS0230	An error occurred while removing the enclosure. Try the operation again. If the failure persists, initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	
HSCS0231	An error occurred while attempting to launch the selected task. Try the operation again. If the failure persists, initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	
HSCS0232	The FRU was successfully added.	
HSCS0233	An error occurred while adding the FRU. Try the operation again. If the failure persists, initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	
HSCS0234	The enclosure was successfully added.	
HSCS0235	An error occurred while adding the enclosure. Try the operation again. If the failure persists, initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	

HSCSxxx error codes	Message	Recovery action
HSCS0236	An error occurred while determining the list of enclosures associated with the system. Try the operation again. If the failure persists, initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	
HSCS0237	An error occurred while determining the list of FRUs contained within the selected enclosure. Try the operation again. If the failure persists, initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	
HSCS0238	An error occurred while determining the list of installed components within the system. Try the operation again. If the failure persists, initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	
HSCS0239	An unexpected error was return from the Repair/Verify subsystem. Contact your service representative.	
HSCS0240	An error occurred while attempting to launch the Information Center task. Try the operation again. If the failure persists, initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	
HSCS0241	An invalid hostname was detected on the HMC. Verify the HMC's network settings and try the operation again.	
HSCS0242	An unrecoverable error has occurred. Could not obtain a CIM client instance. Try the operation again. If the failure persists, initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	
HSCS0243	An unrecoverable error has occurred. No CIM client instance was returned. Try the operation again. If the failure persists, initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required.	
HSCS0244	An unrecoverable error has occurred. The Repair/Verify subsystem could not be invoked.	

HSCSxxx error codes	Message	Recovery action
HSCS0245	An unrecoverable HMC internal error has occurred. Try the operation again. If the failure persists, initiate the 'View Problem Logs' task from the Service Utilities menu for detailed error information. 'hscpe' authority will be required. Contact your service representative.	
HSCS0246	A required parameter is missing to access the remote server. Ensure all required fields are filled in and try the operation again.	
HSCS0247	The specified dump no longer resides on this HMC.	
HSCS0248	The user ID and password combination to log in to the remote server is incorrect. Ensure the combination is valid and try the operation again.	
HSCS0249	An error occurred attempting to change directories on the remote server. Ensure the directory entry is valid and try the operation again.	
HSCS0250	An unrecoverable error occurred while transferring the file to the remote server. Verify the target environment on the remote server can accommodate the request and try the operation again.	
HSCS0251	An error occurred attempting to contact the remote system. Ensure a valid hostname or IP address has been entered and try the operation again.	
HSCS0252	The selected file was successfully copied to the remote server.	
HSCS0253	The managed system is not in the Operating state. Place the system in the correct state and try the operation again.	
HSCS0254	This operation is not allowed when the managed system is in the {0} state. After you have established a connection from the HMC to the managed system and have entered a valid HMC access password, try the operation again.	
HSCS0255	This operation is not allowed when a FRU LED within the selected enclosure is active.	

HSCS _{xxxx} error codes	Message	Recovery action
HSCS0260	Service Processor could not be enabled for failover. Try the operation again at a later time. If the failure persists, view the console events log file for detailed error information.	<ol style="list-style-type: none"> To isolate the type of problem that is occurring, perform the following steps: <ol style="list-style-type: none"> On the HMC, right-click the desktop and select terminal → rshterm. The restricted shell command line interface displays. At the terminal, issue the enable failover command: <pre>chsyscfg -m <system name> -r sys -i sp_failover_enabled=1</pre> Choose from the following options: <ul style="list-style-type: none"> If an error message is received which indicates a <i>half genesis</i> condition exists, continue with step 3. For all other error messages, continue with step 4. Perform the following steps if you received an error message indicating a <i>half genesis</i> condition exists: <ol style="list-style-type: none"> Shutdown the system. When the managed system reaches <i>Power off</i> state, attempt to enable failover. If the problem persists, continue with step 4. Work with your next level of support to perform a service processor dump. They can help you to analyze the results to further isolate the problem.

Virtual terminal errors (Comm) error codes

When using a virtual terminal (VTERM), you might see an error code displayed in the bottom-left corner of the VTERM window. The following table lists the error codes and the recovery actions for each.

Virtual terminal (VTERM) error codes	Message	Recovery action
Comm 654	<p>The virtual terminal server is unable to process this type of request.</p> <p>An unknown error occurred during virtual terminal device-type negotiations.</p>	If the error persists, contact the system administrator for help.
Comm 655	The socket connection to the virtual terminal server has been established and the session is waiting for negotiation to finish.	If the error persists, contact the system administrator for help.
Comm 657	<p>The session is in the process of establishing the TCP/IP connection to the virtual terminal server.</p> <p>When you close a session that displays COMM 657, there might be some delay before it closes.</p>	The delay varies. You can close the browser.
Comm 658	The session is initializing the TCP/IP connection to the HMC.	If the error persists, contact the system administrator for help.

Virtual terminal (VTERM) error codes	Message	Recovery action
Comm 659	The virtual terminal TCP connection to the session has not succeeded or has failed.	<p>One of the following might have occurred:</p> <ul style="list-style-type: none"> • The TCP/IP connection to the virtual terminal server was not established. • Disconnect was selected on the Communication menu. • The virtual terminal server closed the TCP/IP connection either by application control or because it detected an error.

Service request numbers (SRNs)

Service request numbers (SRNs) can appear when AIX online diagnostics or eServer stand-alone diagnostics are run on your server.

If a problem occurs on your server or partition, SRNs might be displayed to indicate that a problem exists. Record any SRNs you receive, and provide them to your hardware service provider. The SRN can be used to help determine what needs to be done to correct the problem. For details on reporting an SRN to your service provider, see “Using the problem reporting forms” on page 443.

Supporting diagnostics

Learn more about procedures that can aid you in analyzing problems.

Occasionally your problem analysis will lead you to more extensive procedures that can help analyze a problem.

Running the online and eServer stand-alone diagnostics

Use these tools to diagnose hardware problems on your AIX or Linux systems or partitions.

Use these diagnostics only if you are directed to do so by your next level of support or your hardware service provider.

Diagnostics are available for AIX and Linux systems or logical partitions which can help you perform hardware analysis. Additionally, there are various service aids in AIX diagnostics that can help you with service tasks on the system or logical partition. If there is a problem, you will receive a Service Request Number (SRN) that can help you pinpoint the problem and determine a corrective action.

If you have AIX installed and it is running, you can perform online diagnostics. However, if the installed AIX cannot be started, or you have Linux installed, you will need to run the diagnostics from CD or from a NIM server.

Running the online diagnostics

If you have AIX installed and it can be started, use this procedure to perform diagnostic procedures when directed from another procedure or by your next level of support.

When you run online diagnostics, keep the following in mind:

- When AIX is installed, the support for some devices might not be automatically installed. If this happens, that device will not display in the test list when online diagnostics run.
- When running diagnostics in a logically partitioned system, you must run diagnostics in the logical partition containing the resource or resources that you want to test.

Three modes are available for running the online diagnostics:

- **Service mode** provides the most complete check of the system resources, but requires that no other programs are running on the system. When possible, run the diagnostics in service mode.
- **Maintenance mode** allows you to check most of the available resources, with the exception of SCSI adapters, memory, processor, and the disk drive used for paging.
- **Concurrent mode** allows you to run online diagnostics on some of the system resources while the system is running normal activity.

Running the online diagnostics in service mode:

Use this procedure to run the online diagnostics in service mode.

Using service mode will check everything except the SCSI adapter and the disk drives used for paging. However, memory and processor are only tested during POST. Running in service mode ensures that the error state of the system that has been captured in NVRAM is available for your use in analyzing the problem.

Running the online diagnostics in service mode with an HMC attached:

Use this procedure to run the online diagnostics in service mode with an HMC attached.

Perform the following steps:

1. Stop all programs including the AIX operating system. For details, see Start or stop the system.
2. From the HMC, right-click **Partition Manager** and select **Open Terminal Window**.
3. From the Service Processor Menu on the VTERM, select option 2 (System Power Control).
4. Select option 6.
5. Verify that the state changes to currently disabled. Disabling fast system boot automatically enables slow boot.
6. Select option 98 to exit the system power control menu.
7. From the HMC, start the managed system in a full system partition by following these steps:
 - a. In the Contents area, select the managed system.
 - b. Right-click, and select **Power On**.
8. Select **Power on Diagnostic Stored Boot list**.
9. Make sure that there is no media in the devices in the media subsystem.
10. Enter any passwords, if requested.
11. When the Diagnostic Operating Instructions screen displays, follow the online instructions to check the desired resources.

Note: If you do not receive the Diagnostic Operating Instructions display, try to run the standalone diagnostics. For details, see “Running the eServer stand-alone diagnostics from CD-ROM” on page 408.

12. When finished, contact your next level of support or your hardware service provider with any information you received during the diagnostics, including service request numbers (SRNs). For details, see the “Using the problem reporting forms” on page 443. **This ends the procedure.**

Running the online diagnostics in service mode without an HMC attached:

Use this procedure to run the online diagnostics in service mode *without* an HMC attached.

Perform the following steps:

1. Stop all programs including the AIX operating system. For details, see Start or stop the system.
2. Remove all tapes, diskettes, and CDs.

3. Turn off the system unit power.
4. Turn on the system unit power.
5. After the keyboard POST indicator displays on the firmware console, and before the last POST indicator (speaker) displays, press 6 on the keyboard or ASCII terminal to indicate that a service mode boot should be initiated using the customized service mode boot list.
6. Enter any passwords, if requested.
7. When the Diagnostic Operating Instructions screen displays, follow the online instructions to check the desired resources.

Note: If you do not receive the Diagnostic Operating Instructions display, try to run the standalone diagnostics. For details, see “Running the eServer stand-alone diagnostics from CD-ROM” on page 408.

8. When finished, contact your next level of support or your hardware service provider with any information you received during the diagnostics, including service request numbers (SRNs). For details, see the “Using the problem reporting forms” on page 443. **This ends the procedure.**

Running the online diagnostics in maintenance mode:

Use this procedure to run the online diagnostics in maintenance mode.

Maintenance mode requires that all activity on the logical partition running the AIX operating system be stopped so that the online diagnostics have most of the resources available. All of the system resources, except the SCSI adapters, memory, processor, and the disk drive used for paging can be checked.

Perform the following steps to run the online diagnostics in maintenance mode:

1. Stop all programs running on the logical partition except the AIX operating system. For details, see Start or stop the system. If you need help, contact the system administrator.
2. Log in to the AIX operating system as root user or use CE login.
3. Type the shutdown -m command to stop all activity on the AIX operating system and put it into maintenance mode.
4. When a message indicates that the system is in maintenance mode, enter the diag command to invoke the diagnostic controller so you can run the diagnostics.

Note: It might be necessary to set TERM type again.

5. Enter any passwords, if requested.
6. When the Diagnostic Operating Instructions screen displays, follow the online instructions to check the desired resources.

Note: If you do not receive the Diagnostic Operating Instructions display, try to run the standalone diagnostics. For details, see “Running the eServer stand-alone diagnostics from CD-ROM” on page 408.

7. When finished, press Ctrl+D to log off from root user or CE login.
8. Contact your next level of support or your hardware service provider with any information you received during the diagnostics, including service request numbers (SRNs). For details, see the “Using the problem reporting forms” on page 443. **This ends the procedure.**

Running the online diagnostics in concurrent mode:

Use this procedure to run the online diagnostics in concurrent mode.

Use concurrent mode to run online diagnostics on some of the system resources while the system is running normal activity.

Because the system is running in normal operation, the following resources cannot be tested in concurrent mode:

- SCSI adapters connected to paging devices
- Disk drive used for paging
- Some display adapters and graphics related devices

The following levels of testing exist in concurrent mode:

Share-test level

This level tests a resource while the resource is being shared by programs running in the normal operation. This testing is mostly limited to normal commands that test for the presence of a device or adapter.

Sub-test level

This level tests a portion of a resource while the remaining part of the resource is being used in normal operation. For example, you could test one port of a multiport device while the other ports are being used in normal operation.

Full-test level

This level requires the device to not be assigned or used by any other operation. This level of testing on a disk drive might require the use of the vary off command. Use the diagnostics display menus to allow you to vary off the needed resource.

Perform the following steps to run online diagnostics in concurrent mode:

1. Log in to the AIX operating system as root user, or use CE login. If you need help, contact the system administrator.
2. Enter the diag command to load the diagnostic controller, and display the online diagnostic menus.
3. If requested, enter a password.
4. When the Diagnostic Operating Instructions screen displays, follow the online instructions to check the desired resources.

Note: If you do not receive the Diagnostic Operating Instructions display, try to run the standalone diagnostics. For details, see “Running the eServer stand-alone diagnostics from CD-ROM.”

5. When testing is complete, press F3 to return to the Diagnostic Operating Instructions display.
6. Press F3 again to return to the AIX operating system prompt.
7. Vary on any resources that you varied off.
8. Press Ctrl+D to log off from root user or CE login.
9. When finished, contact your next level of support or your hardware service provider with any information you received during the diagnostics, including service request numbers (SRNs). For details, see the “Using the problem reporting forms” on page 443. **This ends the procedure.**

Running the eServer stand-alone diagnostics from CD-ROM

If the system or logical partition where you would like to run diagnostics has AIX installed but it cannot be started, or you have Linux installed, use this procedure to perform diagnostic procedures from CD-ROM when directed from another procedure or by your next level of support.

Diagnostics, which are available for AIX and Linux systems and logical partitions, can help you perform hardware analysis. If a problem is found, you will receive a service request number (SRN) or a service reference code (SRC) that can help pinpoint the problem and determine a corrective action.

Additionally, there are various service aids in the diagnostics that can help you with service tasks on the system or logical partition.

Running the eServer stand-alone diagnostics from CD on a server with an HMC attached:

Learn how to run the eServer stand-alone diagnostics on a system with an HMC attached.

If you have logical partitions, note the following considerations:

- When running diagnostics in a logically partitioned system, you must run diagnostics in the logical partition containing the resource or resources that you want to test.
- The device from which you are loading stand-alone diagnostics must be made available to the logical partition on which you want to run diagnostics. This might require moving the device (for example, the CD drive or network adapter connected to the Network Installation Management (NIM) server that has a stand-alone diagnostic image) from the logical partition that currently contains the device to the logical partition on which you want to run diagnostics.

Perform the following steps from the HMC to run stand-alone diagnostics:

Note: If you need help with any of these steps, contact your system operator.

1. Remove all tapes, diskettes, CDs, or DVDs, and insert the diagnostic CD into the CD drive on the managed system (not the CD drive on the HMC).
2. Shut down the operating system from the HMC by performing the following steps:
 - a. In the navigation area, select **Server and partition** → **Server Management**.
 - b. In the contents pane, expand the server that contains the partition you want to test.
 - c. Right-click the partition and select **Open Terminal Window**.
 - d. In the VTerm window, log in as root user and enter any requested passwords.
 - e. Shut down the operating system using one of the following commands:
 - If AIX is running, type the shutdown -F command.
 - If Linux is running, type the shutdown -h now command
 - f. Close the VTerm window.
3. From the HMC, right-click the partition and select **Activate**.
4. Ensure the **Open a terminal window or console session box** is selected and click **OK**.
5. When the keyboard POST indicator (the word *keyboard*) is shown on the firmware console, and before the last POST indicator (the word *speaker*) is shown, press the 5 key on either the attached keyboard or the ASCII keyboard to indicate that a service mode boot should be initiated using the default service mode boot list.
6. Continue with "Selecting testing options."

Selecting testing options:

1. When the keyboard POST indicator (the word *keyboard*) is shown on the firmware console, and before the last POST indicator (the word *speaker*) is shown, press the 5 key on either the attached keyboard or the ASCII keyboard to indicate that a service mode boot should be initiated using the default service mode boot list.
2. When the Welcome screen is shown, define the following:
 - System console
 - Language to be used
 - Type of terminal

Note: Depending on the terminal emulator selected, the function keys (Fn) might not function. In this case, use the ESC and the number in the screen menus. For example, F3 = ESC key and the #3.

3. When the Diagnostics Operating Instructions appear, press Enter.

Note: If you are unable to load the diagnostics to the point where the "Diagnostic Operating Instructions" display is shown, contact your next level of support or your hardware service provider.

4. From the Function Select screen, select one of the following:
 - If you want to run diagnostics in Problem Determination mode, continue with the next step.
 - If you want to run diagnostics in Task Selection (Service Aids) mode, go to step 11.
5. Select **Problem determination** and press Enter.
6. Check the list of resources that is displayed. Does the list of resources match what you know to be installed in your system or partition?
 - **Yes:** Continue with the next step.
 - **No:** Record any information you have about the missing resource and check to ensure that the missing resource is installed correctly. If you cannot correct the problem with a missing resource, replace the missing resource (contact your service provider if necessary). To test the available resources, continue with the next step.
7. Select **All Resources**, or the specific resource or resources to be tested, and press the P7 (commit) key.
8. Record any error information you receive during the diagnostics, including service request numbers (SRNs) or SRCs, to report to your service provider. For details, see “Using the problem reporting forms” on page 443.
9. When testing is complete, press the F3 key to return to the Diagnostic Operating Instructions.
10. Choose from the following options:
 - To continue testing, return to step 7.
 - To exit stand-alone diagnostics, select the exit function key from the menu and press Enter. Continue with step 18.
11. Select **Task Selection list** and press Enter.
12. To perform one of these tasks, select the **Task Selection** option from the Function Selection menu. After a task is selected, a resource menu might be presented showing all resources supported by the task.
13. From the Task selection list, select the service aid task you want to perform. For example, Update and manage system Flash.
14. Follow the instructions for the task selected on each menu or panel.
15. Record any information you receive during the diagnostics, including service request numbers (SRNs), to report to your service provider. For details, see the “Using the problem reporting forms” on page 443.
16. When testing is complete, press the F3 key to return to the Diagnostic Operating Instructions.
17. Choose from the following options:
 - To continue testing, return to step 13.
 - To exit stand-alone diagnostics, select the exit function key from the menu and press Enter. Continue with the next step.
18. Remove the CD from the drive.
19. When finished, contact your next level of support or your hardware service provider with any information you received during the diagnostics, including service request numbers (SRNs) and any missing resources. For details, see the “Using the problem reporting forms” on page 443. **This ends the procedure.**

Running the eServer stand-alone diagnostics from CD on a server without an HMC attached:

Learn how to run the eServer stand-alone diagnostics on a system without an HMC attached.

1. Choose from the following options:
 - If the system is powered on, continue with step 2.
 - If the system is powered off, continue with step 3 on page 411.
2. If the system is powered on, perform these steps:

- a. Let the system administrator and system users know that the system unit will be shut down.
- b. Stop all programs including the operating system. For details, see Start or stop the system.
- c. Continue with step 4.
3. If the system is powered off, perform the following steps:
 - a. Start the server so you will be able to insert the diagnostic CD into the CD drive during the next step.
 - b. Continue with step 4.
4. Insert the diagnostic CD in the CD drive.
5. Restart the server.
6. Continue with "Selecting testing options."

Selecting testing options:

1. When the keyboard POST indicator (the word *keyboard*) is shown on the firmware console, and before the last POST indicator (the word *speaker*) is shown, press the 5 key on either the attached keyboard or the ASCII keyboard to indicate that a service mode boot should be initiated using the default service mode boot list.
2. When the Welcome screen is displayed, define the following:
 - System console
 - Language to be used
 - Type of terminal

Note: Depending on the terminal emulator selected, the function keys (Fn) might not function. In this case, use the ESC key and the number in the screen menus. For example, F3 = ESC key and the #3.
3. When the Diagnostics Operating Instructions appear, press Enter.

Note: If you are unable to load the diagnostics to the point where the Diagnostic Operating Instructions display is shown, contact your next level of support or your hardware service provider.
4. From the Function Select screen, select one of the following:
 - If you want to run diagnostics in Problem Determination mode, continue with the next step.
 - If you want to run diagnostics in Task Selection (Service Aids) mode, go to step 11 on page 412.
5. Select **Problem determination** and press Enter.
6. Check the list of resources that is displayed. Does the list of resources match what you know to be installed in your system or partition?
 - **Yes:** Continue with the next step.
 - **No:** Record any information you have about the missing resource and check to ensure that the missing resource is installed correctly. If you cannot correct the problem with a missing resource, replace the missing resource (contact your service provider if necessary). To test the available resources, continue with the next step.
7. Select **All Resources**, or the specific resource or resources to be tested, and press the P7 (commit) key.
8. Record any error information you receive during the diagnostics, including service request numbers (SRNs) or SRCs, to report to your service provider. For details, see "Using the problem reporting forms" on page 443.
9. When testing is complete, press the F3 key to return to the Diagnostic Operating Instructions.
10. Choose from the following options:
 - To continue testing, return to step 7.
 - To exit stand-alone diagnostics, select the exit function key from the menu and press Enter. Continue with step 19 on page 412.

11. Select **Task Selection list** and press Enter.
12. To perform one of these tasks, select the **Task Selection** option from the Function Selection menu. After a task is selected, a resource menu might be presented showing all resources supported by the task.
13. From the Task selection list, select the service aid task you want to perform. For example, Update and manage system Flash.
14. Follow the instructions for the task selected on each menu or panel.
15. Record any information you receive during the diagnostics, including service request numbers (SRNs), to report to your service provider. For details, see the “Using the problem reporting forms” on page 443.
16. Record any information you receive during the diagnostics, including service request numbers (SRNs), to report to your service provider. For details, see the “Using the problem reporting forms” on page 443.
17. When testing is complete, press the F3 key to return to the Diagnostic Operating Instructions.
18. Choose from the following options:
 - To continue testing, return to step 13.
 - To exit stand-alone diagnostics, select the exit function key from the menu and press Enter. Continue with the next step.
19. Remove the CD from the drive.
20. When finished, contact your next level of support or your hardware service provider with any information you received during the diagnostics, including service request numbers (SRNs) and any missing resources. For details, see the “Using the problem reporting forms” on page 443. **This ends the procedure.**

Running the eServer stand-alone diagnostics from a Network Installation Management server

If the system or logical partition where you would like to run diagnostics has AIX installed but it cannot be started, or you have Linux installed, use this procedure to perform diagnostic procedures from a Network Installation Management (NIM) server when directed from another procedure or by your next level of support.

Diagnostics, which are available for AIX and Linux systems and logical partitions, can help you perform hardware analysis. If a problem is found, you will receive a service request number (SRN) that can help pinpoint the problem and determine a corrective action.

A client system connected to a network with a NIM server can boot stand-alone diagnostics from the NIM server if the client-specific settings on both the NIM server and client are correctly configured.

Notes:

- For NIM clients that have adapters that would typically require that supplemental media be installed when stand-alone diagnostics are run from CD, the support code for these adapters must be installed into the directory pointed to by the NIM SPOT from which you want to boot that client. Before running stand-alone diagnostics on these clients from the NIM server, the NIM server system administrator must ensure that any needed support for these devices is installed on the server.
- All operations to configure the NIM server require root user authority.
- If you replace the network adapter in the client, the network adapter hardware address settings for the client must be updated on the NIM server.
- Ensure that the **Cstate** for each stand-alone diagnostics client on the NIM server is kept in the *diagnostic boot has been enabled* state.
- On the client system, the NIM server network adapter should be put in the bootlist after the boot disk drive. This allows the system to boot in stand-alone diagnostics from the NIM server if there is a

problem booting from the disk drive. Refer to the Multiboot section under "SMS" in the client system's service guide for information about setting the bootlist.

Configuring the NIM server

Refer to the "Performing advanced NIM configuration tasks" chapter of the AIX Installation and Migration guide for information about performing the following tasks:

- Registering a client on the NIM server
- Enabling a client to run diagnostics from the NIM server

To verify that the client system is registered on the NIM server and the diagnostic boot is enabled, run the command from the command line on the NIM server: `lsnim -a Cstate -z ClientName`. Refer to the following table for system responses.

Note: The ClientName is the name of the system on which you want to run stand-alone diagnostics.

System response	Client status
#name:Cstate:ClientName:diagnostic boot has been enabled:	The client system is registered on the NIM server and enabled to run diagnostics from the NIM server.
#name:Cstate:ClientName:ready for a NIM operation:or #name:Cstate:ClientName:BOs installation has been enabled:	The client is registered on the NIM server but not enabled to run diagnostics from the NIM server. Note: If the client system is registered on the NIM server but Cstate has not been set, no data will be returned.
0042-053 lsnim: there is no NIM object named "ClientName"	The client is not registered on the NIM server.

Configuring the client and running the stand-alone diagnostics from a NIM server

Perform the following steps to run stand-alone diagnostics on a client from the NIM server:

1. Let the system administrator and system users know that the system unit might be shut down.
2. Stop all programs including the AIX or Linux operating system. For details, see Start or stop the system. If you need help, contact the system administrator.
3. Remove all tapes, diskettes, and CDs.
4. Choose from the following options:
 - If you are running stand-alone diagnostics in a full system partition profile, verify with the system administrator and system users that the system unit can shut down using the shutdown command. Then power down the system.
 - If you are running on a logically partitioned system, make sure the CD drive is available to the partition used to run stand-alone diagnostics. Verify with the system administrator and system users using that partition that all applications on that partition must be stopped, and that the partition will be restarted. Stop all programs on that partition, including the operating system.
5. Choose from the following options:
 - If you are in a full system partition, power on the system unit to run stand-alone diagnostics.
 - If you are in a logically partitioned system, restart the partition to run stand-alone diagnostics.
6. When the keyboard indicator is displayed (the word *keyboard* on an HMC virtual terminal window or the keyboard icon on a graphical display) press the number 1 key on the keyboard to display the SMS menu.
7. Enter any requested passwords.
8. Select **Set Up Remote IPL** (Initial Program Load).
9. Enter the client address, server address, gateway address, if applicable, and subnet mask. If there is no gateway between the NIM server and the client, set the gateway address to 0.0.0.0.

To determine if there is a gateway, either ask the system network administrator or compare the first three octets of the NIM server address and the client address. If they are the same, (for example, if the NIM server address is 9.3.126.16 and the client address is 9.3.126.42, the first 3 octets (9.3.126) are the same), then set the gateway address in the RIPL field to 0.0.0.0.

Note: The RIPL is located under the Utility menu in System Management Services (SMS). Refer to it for information about setting these parameters.

10. If the NIM server is set up to allow pinging from the client system, use the ping utility in the RIPL utility to verify that the client system can ping the NIM server.
11. Under the ping utility, choose the network adapter that provides the attachment to the NIM server to do the ping operation. If the ping returns with an OK prompt, the client is prepared to boot from the NIM server. If ping returns with a FAILED prompt, the client cannot proceed with the NIM boot.

Note: If the ping fails, refer to the "Troubleshooting NIM" section of the AIX Installation and Migration guide

12. Exit the SMS Main screen.
13. Select **Select Boot Options** → **Install or Boot a Device** → **Network**.
14. Record the current bootlist settings. You will need to set the bootlist back to the original settings after running diagnostics from the NIM server.
15. Change the bootlist so the network adapter attached to the NIM is first in the bootlist.
16. Set the network parameters for the adapter from which you want to boot.
17. Exit completely from SMS. The system will start loading packets while doing a bootp from the network.
18. Follow the on-screen instructions.
 - If Diagnostic Operating Instructions Version x.x.x displays, stand-alone diagnostics have installed successfully.
 - If the AIX login prompt displays, stand-alone diagnostics did not load. Continue with step 19.
19. If the diagnostics did not load, check the following items:
 - The bootlist on the client might be incorrect.
 - Cstate on the NIM server might be incorrect.
 - Network problems might be preventing you from connecting to the NIM server.
 - Verify the settings and the status of the network. If you continue to have problems, refer to the Boot problems/concerns section for the system unit. Then follow the steps for network boot problems.
20. After running diagnostics, restart the system and use SMS to change the IP settings and bootlist sequence back to the original settings.

Performing a slow boot

Learn how to perform a slow boot using the HMC, control panel, or ASMI menus depending on your configuration.

In some cases, you need to perform a slow-mode boot in order to perform extended diagnostic testing.

Note: A slow-mode boot might yield a new reference code on the control panel, or new errors in the service processor error log. When the server reports a new error code, record it for use in subsequent steps.

Using the HMC to perform a slow boot

Learn how to perform a slow boot using the HMC.

In some cases, you need to perform a slow-mode boot in order to perform extended diagnostic testing.

Note: A slow-mode boot might yield a new reference code on the control panel, or new errors in the service processor error log. When the server reports a new error code, record it for use in subsequent steps.

1. Record any reference codes appearing on the control panel or HMC. See “Collecting reference codes and system information” on page 260 for details.
2. Shut down all logical partitions and the server. For instructions, see Powering off the managed system.
3. In the navigation area, select **Server and Partitions** → **Server Management**.
4. Select the server you want to perform a slow boot on.
5. Select **Selected** → **Properties**.
6. Click the **Power-On Parameters** tab.
7. Under Advanced Options click **show details**.
8. Record the current boot setting in the Power-on speed override box.
9. Select **slow** in the Power-on speed override list.

Note: These settings will apply to all future boots. After you complete the service action, change the settings back to what you recorded in step 8.

10. Click **OK**.
11. After you are done, return to the step in the procedure that caused you to perform a slow boot. **This ends the procedure.**

Using the control panel to perform a slow boot

Learn how to use the control panel to perform a slow boot.

In some cases, you need to perform a slow-mode boot in order to perform extended diagnostic testing.

Note: A slow-mode boot might yield a new reference code on the control panel, or new errors in the service processor error log. When the server reports a new error code, record it for use in subsequent steps.

1. Record any reference codes that are displayed on the control panel. For details, see “Collecting reference codes and system information” on page 260.
2. Stop the operating system by performing the following steps:
 - a. Log in to the system as a user with the authority to run the shutdown or pwrdownsys (Power Down System) command.
 - b. At the command line, enter one of the following commands:

Note: These commands stop the operating system. The system power turns off, the power-on light begins to slowly blink, and the system goes into a standby state.

- If your system is running AIX, type shutdown
 - If your system is running IBM i5/OS, type pwrdownsys *immed
 - If your system is running Linux, type shutdown -h now
3. On the control panel, use the increment or decrement buttons to scroll to function 02.
 4. Press Enter to start function 02. The current IPL type (with pointer) and speed is displayed.
 5. Use the increment or decrement buttons to scroll through the IPL types and speeds.

6. When manual is shown, press Enter to select the IPL type of manual. The current IPL type and speed (with pointer) is displayed.
7. Use the increment or decrement buttons to scroll through the IPL speeds.
8. When S is shown, press Enter to select the IPL speed of slow.
9. To exit function 02, press Enter multiple times until just 02 is displayed.
10. Power on the server by pressing the white power button. Then return to the procedure that caused you to perform a slow boot. **This ends the procedure.**

Using the ASMI menus to perform a slow boot

Learn how to use the ASMI menus to perform a slow boot.

In some cases, you need to perform a slow-mode boot in order to perform extended diagnostic testing.

Note: A slow-mode boot might yield a new reference code on the control panel, or new errors in the service processor error log. When the server reports a new error code, record it for use in subsequent steps.

1. Record any reference codes appearing on the control panel or HMC. For details, see “Collecting reference codes and system information” on page 260.
2. Shut down all logical partitions and the server. For details, see the Powering off the managed system topic.
3. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
4. Expand **Power/Restart Control** and select **Power On/Off System**.
5. Record the settings so that you can re-enter them after you complete the service actions.
6. On the Power on/off system menu, select the following:
 - Select **Slow** in the Set System Boot Speed field.
 - Select **Running** in the Boot to system server firmware field.
7. Select **Save Settings**.

Note: These settings will apply to all future boots. After you complete the service action, change the settings back to what you recorded in step 5.

8. After you are done, return to the step in the procedure that caused you to perform a slow boot. **This ends the procedure.**

Performing dumps

Learn more about the different types of dumps that can be performed and how to manage them, including copying, reporting, and deleting them.

Dumps can occur automatically after a failure or external reset, or after a manual request. The dump information provides valuable information on system status and should be reported to your next level of support or your hardware service provider.

There are many types of dumps that can be performed, including:

- **System dump**
- **Service processor dump**
- **i5/OS main storage dump (MSD)**

In addition, there are other dumps that generate automatically. These include:

- **Platform event log entry dumps**, which are generated by server firmware when a platform event log entry is truncated
- **Resource dumps**
- **SMP dumps**

Performing a system dump

A system dump is a collection of data from server hardware and firmware, either after a system failure or a manual request.

Perform a system dump only under the direction of your next level of support or your service provider, after first providing to your next level of support or service provider a dump of the operating system (for example, a main storage dump for i5/OS).

Note: Before performing a system dump, collect any reference code information from the control panel or the HMC. For details, see “Collecting reference codes and system information” on page 260.

Using the HMC to perform a system dump:

If your next level of support or your service provider suspects a wait or loop in the server firmware, they might request that you perform a system dump. You can use the HMC to perform a system dump, which is a collection of data from the server hardware and firmware.

Use this procedure only under the direction of your next level of support or your service provider, after first providing to your next level of support or service provider a dump of the operating system (for example, a main storage dump for i5/OS).

Follow these steps to initiate a system dump in Service Focal Point:

1. Perform a controlled shutdown of all partitions.

Note: A system dump will abnormally terminate any running partitions.

2. In the navigation area, open **Service Applications**.
3. Select **Service Focal Point**.
4. Select **Service Utilities**.
5. Select **System Processor**.
6. Select **Selected > Manage dumps**.
7. Select **Action > Initiate System Dump**. The dump is automatically saved to the HMC.
8. For details on how to copy, report, or delete a dump after you have completed a dump, refer to “Managing dumps” on page 420.

Using the control panel to perform a system dump:

If your next level of support or your service provider suspects a wait or loop in the server firmware, they might request that you perform a system dump. If you do not have an HMC, you can use the control panel to perform a system dump, which is a collection of data from the server hardware and firmware.

Use this procedure only under the direction of your next level of support or your service provider, after first providing to your next level of support or service provider a dump of the operating system (for example, a main storage dump for i5/OS).

If you do not have an HMC, follow these steps to perform a system dump:

1. Perform a controlled shutdown of the operating system.

Attention: A platform system dump will abnormally terminate any running partitions.
2. On the control panel, select Manual mode.
3. Use the increment or decrement buttons to select function 42 (system dump).
4. Press Enter on the control panel.
5. Is 00000000 or FF displayed on the control panel for more than 30 seconds?

- **Yes:** The service processor or server firmware is not responding to a request from the control panel. Contact your next level of support or your hardware service provider. **This ends the procedure.**
 - **No:** An attention SRC A1xx3042 is displayed, which indicates that function 42 has been selected.
6. Perform the following steps:
 - a. Reselect function 42 and press Enter on the control panel.
 - b. Return to Normal mode and wait for the dump to complete.
 - c. Wait for the system to IPL again.
 7. For details on how to copy, report, or delete a dump after you have completed a dump, refer to “Managing dumps” on page 420.

Using the ASMI to perform a system dump:

If your next level of support or your service provider suspects a wait or loop in the server firmware, they might request that you perform a system dump. You can use the ASMI to perform a system dump, which is a collection of data from the server hardware and firmware.

Use this procedure only under the direction of your next level of support or your service provider, after first providing to your next level of support or service provider a dump of the operating system (for example, a main storage dump for i5/OS).

To perform a system dump, see Initiating a system dump.

Performing a service processor dump

A service processor dump is a collection of data from a service processor either after a failure, external reset, or manual request.

Perform a service processor dump only under the direction of your next level of support or your service provider, after first providing to your next level of support or service provider a dump of the operating system (for example, a main storage dump for i5/OS).

Using the HMC to perform a service processor dump:

A service processor dump is a collection of data from a service processor either after a failure, external reset, or manual request. You can use the HMC to perform a service processor dump.

Use this procedure only under the direction of your next level of support or your service provider, after first providing to your next level of support or service provider a dump of the operating system (for example, a main storage dump for i5/OS).

Follow these steps to initiate a service processor dump in Service Focal Point:

1. In the navigation area, open **Service Applications**.
2. Select **Service Focal Point**.
3. Select **Service Utilities**.
4. Select **System Processor**.
5. Select **Selected > Manage dumps**.
6. Select **Action > Request SP Dump**. The dump is automatically saved to the HMC.
7. For details on how to copy, report, or delete a dump after you have completed a dump, refer to “Managing dumps” on page 420.

Using the control panel to perform a service processor dump:

A service processor dump is a collection of data from a service processor either after a failure, external reset, or manual request. If you do not have an HMC, you can use the control panel to perform a service processor dump.

Use this procedure only under the direction of your next level of support or your service provider, after first providing to your next level of support or service provider a dump of the operating system (for example, a main storage dump for i5/OS).

If you do not have an HMC, follow these steps to perform a service processor dump:

1. On the control panel, select Manual mode.
2. Use the increment or decrement buttons to select function 43 (service processor dump).
3. Press Enter on the control panel.
4. Is 00000000 or FF displayed on the control panel for more than 30 seconds?
 - **Yes:** The service processor or server firmware is not responding to a request from the control panel. Contact your next level of support or your hardware service provider. **This ends the procedure.**
 - **No:** An attention SRC A1xx 3043 is displayed, which indicates that function 43 has been selected.
5. Perform the following steps:
 - a. Reselect function 43 and press Enter on the control panel.
 - b. Return to Normal mode, and wait for the dump to complete.
6. For details on how to copy, report, or delete a dump after you have completed a dump, refer to “Managing dumps” on page 420.

Using the ASMI to perform a service processor dump:

A service processor dump is a collection of data from a service processor either after a failure, external reset, or manual request. You can use the ASMI to perform a service processor dump.

Use this procedure only under the direction of your next level of support or your service provider, after first providing to your next level of support or service provider a dump of the operating system (for example, a main storage dump for i5/OS).

To perform a service processor dump, see Initiating a service processor dump.

Performing an IBM i5/OS main storage dump

A main storage dump is a collection of data from the i5/OS's main storage. It can be manually initiated when the system administrator suspects a system wait or loop, or automatically by the server firmware as the result of a system failure.

Note: Before performing a main storage dump, collect any reference code information from the control panel or the HMC. For details, see “Collecting reference codes and system information” on page 260.

Using the HMC to perform an IBM i5/OS main storage dump:

Learn how to use the HMC to perform an IBM i5/OS main storage dump.

Note: Before performing a or main storage dump, collect any reference code information from the control panel or the HMC. For details, see “Collecting reference codes and system information” on page 260.

Follow these steps to perform a main storage dump from an HMC:

Note: If a main storage dump occurred automatically, go to “Managing dumps” on page 420 for information on how to copy, report, or delete a dump.

1. In the navigation area, open **Server and Partition**.

2. Select **Server Management**.
3. In the contents area, expand Partitions.
4. Right-click the logical partition and select **Restart Partition**.
5. Select **Dump**.
6. Click **OK**.
7. For details on how to copy, report, or delete a dump after you have completed a dump, refer to "Managing dumps."

Using the control panel to perform an IBM i5/OS main storage dump:

Learn how to use the control panel to perform an IBM i5/OS main storage dump.

Note: Before performing a or main storage dump, collect any reference code information from the control panel or the HMC. For details, see "Collecting reference codes and system information" on page 260.

If you do not have an HMC, follow these steps to perform a platform system dump:

1. Verify that no interactive jobs are running.
2. On the control panel, select Manual mode.
3. Use the increment or decrement buttons to select function 22 (main storage dump).
4. Press Enter on the control panel.
5. Is 00000000 or FF displayed on the control panel for more than 30 seconds?
 - **Yes:** The service processor or server firmware is not responding to a request from the control panel. Contact your next level of support or your hardware service provider. **This ends the procedure.**
 - **No:** An attention SRC A1xx 3022 is displayed, which indicates that function 22 has been selected. Continue with the next step.
6. Perform the following steps on the control panel:
 - a. Reselect function 22.
 - b. Press Enter.
 - c. Switch back to Normal mode and wait for the dump to complete. If function 22 was selected, the appearance of an A2D0 3000 on the console indicates that a successful user-initiated main storage dump was performed. (A B6xx xxxx reference code indicates that a successful i5/OS initiated main storage dump was performed.)
7. For details on how to copy, report, or delete a dump after you have completed a dump, refer to "Managing dumps."

Virtual I/O Server dumps

Learn how to manage Virtual I/O Server dumps using the Integrated Virtualization Manager.

For details on managing dumps for a Virtual I/O Server, see "Managing dumps with Service Focal Point for the Integrated Virtualization Manager" on page 441.

Managing dumps

After you have performed a dump, or one occurs automatically, use this information to manage the dump, including copying, reporting, and deleting it.

Dumps are deleted automatically when a new dump occurs, except for log dumps.

Copying a dump:

Use this procedure to copy a current platform dump or current main storage dump when the Main Storage Dump auto copy option is disabled. Copying the current dump allows another dump of the same type to be created.

Note: If you have an HMC, you must manage your platform dumps with the HMC. However, you will need to manage i5/OS main storage dumps with the IBM i5/OS service tools.

Using an HMC to copy a dump:

Learn how to copy a dump using an HMC.

Note: If you have an HMC, you must manage your platform dumps with the HMC. However, you will need to manage i5/OS main storage dumps with the IBM i5/OS service tools.

1. In the navigation area, open **Service Applications**.
2. Select **Service Focal Point**.
3. Select **Service Utilities**.
4. Select **System Processor**.
5. Select **Selected > Manage Dumps**.
6. Select the dump to copy.
7. Verify the **HMC containing dump** is the HMC being used to copy the dump.
8. To copy the dump to DVD media, select **Selected > Copy Dump File to DVD Media**.
9. Load the media and follow the instructions on the display.
10. When the copy procedure is successfully completed, remove the media and process it according to the instructions of your next level of support or your hardware service provider.
11. If you encounter a problem with the copy procedure, contact your next level of support or your hardware service provider. **This ends the procedure.**

Using the AIX command line to copy a dump:

Learn how to use the AIX command line to copy a dump.

Copy the dump only if you are directed to do so by your next level of support or service provider.

Note: If you have an HMC, you must manage your platform dumps with the HMC. For details, see “Using an HMC to copy a dump.”

Platform dumps are saved in AIX under the following directory:

`/var/adm/platform`

Note: If the AIX partition becomes the service partition after it was installed, run the following command to create this directory:

```
platform_dump -f jfs2
```

or

```
platform_dump -f jfs
```

This command will create the `/var/adm/ras/platform` file system. This is done automatically during installation if the AIX partition was marked as the service partition before it was installed.

Using the IBM i5/OS service tools to copy a dump:

Learn how to use the i5/OS service tools to copy a dump.

Choose from the following options:

- To copy a platform system or SP dump, go to “Copying a platform system or SP dump” on page 422.
- To copy a main storage dump, go to “Copying a main storage dump” on page 422.

Copying a platform system or SP dump:

Use this procedure to copy a platform system or SP dump with the i5/OS tools.

Note: If you have an HMC, you must manage your platform dumps with the HMC. For details, see “Using an HMC to copy a dump” on page 421.

1. On any command line, enter STRSST.

Note: For details on accessing a 5250 console session on an HMC, see Managing the HMC 5250 Console.

2. Enter a valid service tools user ID and password.
3. Select option 1 (Start a service tool).
4. Select option 6 (Main storage dump manager). Did option 7 (Work with current platform dump) appear on the Main Storage Dump Manager display?
 - **Yes:** There is a current platform dump. Continue with the next step.
 - **No:** There is no current platform dump. A dump might have been automatically copied to the Auxiliary Storage Pool (ASP). Go to Reporting a dump. **This ends the procedure.**
5. Select option 7 (Work with current platform dump).
6. Select option 1 (Display summary). The Platform Dump Summary display shows the platform dump type, date and time of the dump, and reference code.
7. Record the summary information and report it to your next level of support or your hardware service provider.
8. Press F12 (Cancel).
9. Select option 3 (Copy to ASP). The platform dump will be copied to disk storage. After the dump is copied, a message will be displayed indicating whether the copy completed.
10. Did a message indicate “Copy completed normally”?
 - **Yes:** There no longer is an option 7 (Work with current platform dump) listed. **This ends the procedure.**
 - **No:** Continue with the next step.
11. Has your next level of support or your hardware service provider requested a media copy of the platform dump?
 - **Yes:** Continue to the next step.
 - **No:** Work with your next level of support or your hardware service provider on the problem. **This ends the procedure.**
12. If the copy to disk failed, copy a current platform dump to removable media by performing the following steps:
 - a. Select option 2 (Copy to media).
 - b. Load the media and follow the instructions on the display.
 - c. When the copy procedure is successfully completed, remove the media and process it according to the instructions of your next level of support or your hardware service provider.
13. If you encounter a problem with the copy procedure, contact your next level of support or your hardware service provider. **This ends the procedure.**

Copying a main storage dump:

Use this procedure to copy an i5/OS main storage dump using i5/OS tools.

1. On any command line, enter STRSST.

Note: For details on accessing a 5250 console session on an HMC, see Managing the HMC 5250 Console.

2. Enter a valid service tools user ID and password.
3. Select option 1 (Start a service tool).
4. Select option 6 (Main storage dump manager).
5. From the Main Storage Dump Manager display, press Enter.

Note: Copying a main storage dump (MSD) to disk storage on the system prevents the MSD from being overwritten in the event that another MSD occurs.

6. Select option 1 (Display/Print).
7. Select option 1 (MSD summary). The Main Storage Dump Summary display shows the system reference code, date and time of the MSD, and Licensed Internal Code (LIC) level.
8. Record the summary information and report it to your next level of support or your hardware service provider.
9. Press F12 (Cancel) twice to return to the Work with Current Main Storage Dump display.
10. Select option 3 (Copy to ASP).
11. Type a dump description and then press Enter to start copying the dump. After the dump is copied, a message is displayed indicating whether the MSD copy completed.
12. Did a message indicate "Copy completed normally"?
 - **Yes: This ends the procedure.**
 - **No:** Continue with the next step.
13. Has your service provider requested a media copy of the MSD?
 - **Yes:** Continue to the next step.
 - **No:** Work with your next level of support or your hardware service provider on the problem. **This ends the procedure.**
14. To copy a current MSD to a removable media, perform the following steps:
 - a. Select option 2 (Copy to media).
 - b. Load the media and follow the instruction on the display.
 - c. When the copy procedure completes successfully, remove the media and process it according to your service provider's instructions. If you encounter a problem with the copy procedure, contact your next level of support or your hardware service provider. **This ends the procedure.**

Using the Linux command line to copy a dump:

Learn how to use the Linux command line to copy a dump.

Copy the dump only if you are directed to do so by your next level of support or service provider.

Note: If you have an HMC, you must manage your platform dumps with the HMC. For details, see "Using an HMC to copy a dump" on page 421.

Platform dumps are saved in Linux under the following directory:

`/var/log/dump/`

Reporting a dump:

Find out how to report a dump using the HMC, i5/OS service tools, AIX command line, or Linux command line.

Using an HMC to report a dump:

Learn how to report a dump using an HMC.

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

2. Select **Service Focal Point**.
3. Select **Service Utilities**.
4. Select **System Processor**.
5. Select **Selected** → **Manage dumps**.
6. Verify that **HMC containing dump** is the HMC being used to report the dump.
7. Select **Selected** → **Call Home Dump**. The dump summary display shows the date, time and size of the dump. Report the summary information to your next level of support or your hardware service provider.
8. Has your next level of support or your hardware service provider requested a copy of the dump?
 - **Yes:** Continue to the next step.
 - **No:** Contact your next level of support or your hardware service provider on the problem.
9. To copy a dump to removable media, perform the following steps:
 - a. Select **Copy Dump File to DVD Media**.
 - b. Load the media and follow the instructions on the display.
 - c. When the copy procedure is successfully completed, remove the media and process it according to the instructions of your next level of support or your hardware service provider. If you encounter a problem with the copy procedure, contact your next level of support or your hardware service provider.
10. To copy a dump to another system, perform the following steps:
 - a. Select **Selected** → **Copy Dump File to Other System**.
 - b. Follow the instructions on the display.
 - c. When the copy procedure is complete, contact your next level of support or your hardware service provider.

Using the AIX command line to report a dump:

Learn how to report a dump using the AIX command line.

Report the dump only if you are directed to do so by your next level of support or service provider.

Platform dumps are saved in AIX under the following directory:

`/var/adm/platform`

Note: If the AIX partition becomes the service partition after it was installed, run the following command to create this directory:

```
platform_dump -f jfs2
```

or

```
platform_dump -f jfs
```

This command will create the `/var/adm/ras/platform` file system. This is done automatically during installation if the AIX partition was marked as the service partition before it was installed.

Using the i5/OS service tools to report a main storage or platform system or SP dump:

Learn how to report a dump using the i5/OS service tools.

If your system has the Main Storage Dump enabled for auto copy, your system might have automatically copied the current MSD to the Auxiliary Storage Pool (ASP) using the dump description Auto Copy. Then it might have performed another IPL of the system, or automatically copied a current platform system or SP dumps to ASP using the dump type as part of the dump description.

1. On any command line, enter STRSST.

Note: For details on accessing a 5250 console session on the HMC, see Managing the HMC 5250 console.

2. Enter a valid service tools user ID and password.
3. Select option 1 (Start a service tool).
4. Select option 6 (Main storage dump manager).
5. Select option 2 (Work with copies of main storage dumps).
6. Find a new dump near the bottom of the list, type 5 (Display/Print) next to it, and press Enter.
7. Did the Display Main Storage Dump display appear?
 - **Yes:** This is a main storage dump. Select option 1 (MSD Summary). Continue with the next step.
 - **No:** This is a platform dump. Continue with the next step.
8. Record the summary information so that you can report it to your next level of support or your hardware service provider. The Dump Summary display shows the date and time of the dump, system reference code (SRC) data, and Licensed Internal Code (LIC) level.
9. Press F3 (Exit).
10. If the dump has a description of Auto Copy, rename it so that another auto copy and IPL can occur if necessary.
 - a. Select option 7 (Rename).
 - b. Type a new dump description, and press Enter.
11. Has your next level of support or your hardware service provider requested a media copy of the dump?
 - **Yes:** Continue with the next step.
 - **No:** Contact your next level of support or your hardware service provider on the problem. Continue with Deleting a dump.
12. To copy an MSD or a platform dump to removable media, perform the following steps:
 - a. Select option 8 (Copy to media).
 - b. Load the media and follow the instructions on the display.
 - c. When the copy procedure completes successfully, remove the media and process it according to the instructions from your next level of support or your hardware service provider. If you encounter a problem with the copy procedure, contact your next level of support or your hardware service provider.
13. Continue with Deleting a dump.

Using the Linux command line to report a dump:

Learn how to report a dump using the Linux command line.

Platform dumps are saved in AIX under the following directory: /var/log/dump/

Report the dump only if you are directed to do so by your next level of support or service provider.

Deleting a dump:

Use this procedure to delete a dump when dump copies are no longer needed by your next level of support or your hardware service provider.

Using an HMC to delete a dump:

Learn how to use an HMC to delete a dump.

Dumps are stored in the HMC's Service Focal Point tool and are automatically deleted when room is required for new dumps. Use this procedure when you want to manually delete a dump.

1. In the navigation area, open **Service Applications**.
2. Select **Service Focal Point**.
3. Select **Service Utilities**.
4. Select **System Processor**.
5. Select **Selected** → **Manage Dumps**.
6. Select the dump to delete.
7. Verify that **HMC containing dump** is the HMC being used to delete the dump.
8. Select **Selected** → **Delete Dump**.

Using the AIX command line to delete a dump:

Learn how to delete a dump using the AIX command line.

Platform dumps are saved in AIX under the following directory:

`/var/adm/platform`

Delete the dump only if directed to do so by your next level of support or service provider.

Note: If the AIX partition becomes the service partition after it was installed, run the following command to create this directory:

```
platform_dump -f jfs2
```

or

```
platform_dump -f jfs
```

to create the `/var/adm/ras/platform` file system.

During an installation, this directory is created automatically if the AIX partition was marked as the service partition before it was installed.

Using the i5/OS service tools to delete a dump:

Learn how to delete a dump using the i5/OS service tools.

1. On any command line, enter STRSST.

Note: For details on accessing a 5250 console session on the HMC, see the Managing the HMC 5250 console topic.

2. Enter a valid service tools user ID and password.
3. Select option 1 (Start a service tool).
4. Select option 6 (Main storage dump manager).
5. Select option 2 (Work with copies of main storage dumps).
6. If you want to delete any dump copies, type 4 next to the dump copies, and press Enter twice.
7. To exit SST, press F3 (Exit) three times, and then press Enter.

Using the Linux command line to delete a dump:

Learn how to delete a dump using the Linux command line.

Platform dumps are saved in Linux under the following directory: `/var/log/dump/`

Delete the dump only if directed to do so by your next level of support or service provider.

Determining the primary or alternate console

Use this procedure to determine the primary or alternate console.

If the HMC has been configured as the primary console, the system will start the HMC.

If the Operations Console has been configured as the primary console, the system will start the Operations Console. If the Operations Console has not been configured, the primary console is a workstation that is attached to the first input/output processor (IOP) that is capable of supporting workstations.

In addition to the primary console, the system can assign up to two alternative consoles. The first alternative console can only be a twinax workstation that is attached to the same IOP as the primary console. The second alternative console is a workstation that is attached to the next IOP or input/output adapter (IOA) that is capable of supporting workstations.

The IOP that supports the console must be on the first system bus (bus 1).

If a workstation is not correctly attached to the first IOP that is capable of attaching workstations, then the system will not assign a primary console. The system will display a reference code on the operator's panel. In addition, if the IPL (initial program load) mode is set to Manual, the system will stop.

Primary console workstation requirements

Learn about the primary console workstation requirements.

In order to be the primary console, the workstation must be operational and have the correct port and address. If the workstation is a PC, it must also have an active emulation program on the workstation.

The workstation requirements are:

- HMC
- twinax workstation - Port 0 Address 0
- ASCII workstation - Port 0
- PC attached to ASCII IOP or IOA
 - Port 0
 - PC software to emulate a 316x or 3151 terminal
- PC attached to twinax IOP
 - Port 0 Address 0
 - 5250 emulator software active on PC
- PC attached to a LocalTalk IOA (6054)
 - SNAPS 5250 Version 1.2 (or above) application
 - Console capable selected on Macintosh (IOA converts to Port 0 Address 0)
- PC attached to a 2609, 2612, 2699, or 2721 communications IOA
 - Client Access Console cable attached to the 2609 or 2612 P2 port (part number 46G0450 or 46G0479), 2699 (part number 21H3779), or 2721 (part number 44H7504)
 - Operations Console cable attached to the 2609 or 2612 (part number 97H7555), 2699 (part number 97H7556), or 2721 (part number 97H7557) - 5250 emulation or Rumba active on PC

Find the primary console when the system is operational

Learn how to find the primary console when the system is operational.

The following methods are available to find the primary console:

- **Method 1:** Look for a sign-on display with a DSP01 in the upper-right corner.
- **Method 2:** If the device name (DSP01) for the console has been changed, you can verify the device name for the primary console by doing the following:
 1. Enter DSPCTLD QCTL on any command line. The Display Controller Description display is displayed.
 2. Find the Resource name parameter (such as CTL01) and record it.
 3. Enter PRTDEVADR rrrr on any command line, where rrrr is the resource name you recorded.

Note: If the printer is active, the data will print.

- **Method 3:**
 1. Enter STRSST on any command line. The System Service Tools display is displayed.
 2. Select option 1 (Start a service tool).
 3. Select option 7 (Hardware service manager).
 4. Select option 2 (Logical hardware resources).
 5. Select option 1 (System bus resources). On the Logical Hardware Resources on System Bus display, the "<" symbol indicates the IOP that the console is attached to.
 6. Use option 9 (Resource associate with IOP and display detail) to find the location of the system bus, board, and card.

Find the primary console when the system power is off

Learn how to find the primary console when the system power is off.

Use one of the following:

- Turn on the system in Manual mode and look for the IPL and Install System display.
- Turn on the system in Normal mode and look for DSP01 on the sign on display.

Note that the name might have been changed. See “Find the primary console when the system is operational” on page 427 to determine the display name.

Correcting the managed system operating state

Learn how to correct a *No connection*, *Incomplete*, *Recovery*, or *Error* state on a system managed by an HMC.

Correcting a *No connection* state for a managed system

The *No connection* state can occur when the HMC is not connected, or the handshake with the managed system failed.

Use this procedure for a system that was previously connected to the same HMC and is now in *No connection* state. If you have a new system, a new HMC, or have moved your system to a different HMC, refer to “Correcting a connection problem between the HMC and a managed system” on page 431.

1. Obtain the IP address for the managed system’s service processor by performing the following steps.
 - a. On the HMC, right-click the desktop and select **terminal** → **rshterm**. The restricted shell command line interface displays.
 - b. At the terminal, issue the command: `lssysconn -r all`
Information similar to the following appears:

```
resource_type=sys,type_model_serial_num=9117-570*100729E,sp=unavailable,ipaddr=10.0.0.247,alt_ipaddr=unavailable,state=No Connection,connection_error_code=Connecting 0000-0000-00000000
```
 - c. At the terminal, issue the ping command to the address of the failing system. In the example above you would type: `ping 10.0.0.247`.
2. Choose from the following options:
 - If the ping is successful, go to step 3 on page 429.

- If the ping *is not* successful, go to step 4.
3. If the ping test *is* successful, perform the following steps:
 - a. If your system is equipped with a control panel, ensure that there are no steady (that is, non-scrolling) reference codes displayed on the panel.

Note: A steady reference code could indicate a hardware problem. Contact your next level of support or your hardware service provider.
 - b. Restart the HMC.
 - c. If restarting the HMC does not resolve the problem, contact your next level of support or your hardware service provider.
 4. If the ping test *is not* successful, perform the following steps:
 - a. If your system is equipped with a control panel, ensure that there are no steady (that is, non-scrolling) reference codes displayed on the panel.

Note: A steady reference code could indicate a hardware problem. Contact your next level of support or your hardware service provider.
 - b. If your system has a control panel, check to see if the power light is on.
 - c. Choose from the following options:
 - If there is power to the managed system, go to step 5.
 - If there is no power to the managed system, refer to *Powering on a managed system*. After the power is restored, wait 5 minutes for the service processor to re-IPL and the HMC to re-establish contact. If the system is equipped with redundant service processors, allow up to 20 minutes for this step.
 5. Verify physical network connectivity:
 - a. Verify that the HMC and the service processor are correctly connected to your Ethernet network. For more information, see *Cabling the HMC*.
 - b. Verify that Ethernet link status is good on all network segments which exist between the HMC and the managed system.
 - c. If you think the network might be the problem, connect a cable from the HMC to the service processor and try pinging the failing system. Then choose from the following options:
 - If the ping is successful, put the cables back the way they were and correct the network problem. After the network problem is resolved, repeat this entire procedure.
 - If the ping is not successful, put the cables back the way they were and continue with step 5d.
 - d. Reset the service processor. See “Resetting the service processor” on page 432.
 6. If the problem is not resolved by any of the above steps, contact your next level of support or your hardware service provider.

Correcting an *Incomplete* state for a managed system

The *Incomplete* state can occur when the HMC failed to get all of the necessary information from the managed system.

To correct an *Incomplete* state, perform the following steps:

1. In the HMC's contents area, select the managed system.
2. From the menu, click **Selected > Rebuild Managed System**.
3. Choose from the following options:
 - If the state remains in *Incomplete*, rebuild the managed system several more times.
 - If the state goes to *Recovery*, see “Correcting a *Recovery* state for a managed system” on page 430.
 - If the state does *not* remain in *Incomplete* or go to *Recovery*, continue with the next step.

4. Reset the connection from the HMC. See “Resetting the managed system connection from the HMC” on page 432. If it still fails, continue with the next step.
5. This step might take several minutes to complete. Restart the HMC. Then choose from the following options:
 - If the state goes to *Recovery*, see “Correcting a *Recovery* state for a managed system.”
 - If the state remains *Incomplete*, perform the following steps:
 - a. Verify that there is a redundant HMC.
 - b. Verify that no one is entering commands from the alternate HMC.
 - c. Repeat step 1 on page 429 through 5. If it still fails, continue with the next step.
6. If the problem persists, contact your next level of support or your hardware service provider.

Correcting a *Recovery* state for a managed system

The *Recovery* state can occur when the save area in the service processor assembly is not synchronized with the HMC database.

To recover from the *Recovery* state, perform the following steps:

1. Recover partition data. For details, see Recovering partition data on a managed system. If this solves the problem, this ends the procedure.
2. If the problem is not resolved after recovering profile data, choose the option that describes what happened:
 - If the state remains in *recovery*, retry recovering partition data. If it fails a second time, follow the problem determination procedure for any reference codes you receive.
 - If the state changed to *Incomplete*, refer to “Correcting an *Incomplete* state for a managed system” on page 429.
 - If the state changed to *No Connection*, refer to “Correcting a *No connection* state for a managed system” on page 428.
 - If the problem persists, contact your next level of support or your hardware service provider.

Correcting an *Error* state for a managed system

The *Error* state automatically generates a call to the service support center if the function is enabled.

If the automatic call support function is not enabled, contact your next level of support or your hardware service provider.

Correcting a *Failed Authentication* state for a managed system

The *Failed Authentication* state can occur when the HMC access password for the managed system is not valid.

1. Do you have an HMC password?
 - **Yes:** Enter the HMC password and choose from the following options:
 - If the managed system goes to *Operating*, *Power Off*, or *Standby*, the authentication was successful. **This ends the procedure.**
 - If the managed system goes to *No connection*, *Incomplete*, *Recovery*, or *Error* state, refer to “Correcting the managed system operating state” on page 428.
 - **No:** Do you have an ASMI admin password?
 - **Yes:** Continue with step 2.
 - **No:** Contact your next level of support to request CE login. Then continue with step 2, using CE login instead of admin password for step 2a.
2. Perform the following steps:
 - a. Login to the ASMI with admin authority.
 - b. Select **Login Profile**.

- c. Select **Change Password**.
- d. In the User ID to change field, select **HMC**.
- e. Enter the ASMI's admin password in the Current password for user ID admin field.

Note: Do not enter the HMC user password. Enter the ASMI's *admin* password.

- f. Enter a new HMC access password twice and click **Continue**.
 - g. From the HMC's Server Management window, select **Update the managed system password**.
 - h. Input the new password that was set in step 2f. **This ends the procedure.**
3. If the problem is not resolved by any of the above steps, contact your next level of support or your hardware service provider.

Correcting a connection problem between the HMC and a managed system

Learn how to correct a connection problem between the HMC and a managed system.

Use this procedure in the following situations:

- You have a new HMC
- You have a new system
- You moved your system to a different HMC

If your system was previously connected to the same HMC and is now in *No connection* state, refer to "Correcting a *No connection* state for a managed system" on page 428.

1. Choose from the following options:
 - If the system uses DHCP addressing, go to step 2.
 - If the system uses Static addressing, go to step 6.

Note: To find out if your system uses DHCP or Static addressing, perform one of the following:

- Use the ASMI by selecting **Network Services** → **Network Configuration** and viewing whether the IP address field shows *Static* or *Dynamic*.
 - If you have a control panel, use function 30.
2. If your system uses DHCP addressing, add a system automatically by issuing the following command: `mksysconn -o auto`.
Does the system appear?
 - **Yes: This ends the procedure.**
 - **No:** Continue with step 3.
 3. Check for network problems, cables, switches, link lights on the service processor, and so on.
Was there a problem?
 - **Yes:** Correct the problem and return to step 2.
 - **No:** Continue with step 4.
 4. Reset the service processor to force it to request a new IP address. Refer to "Resetting the service processor" on page 432.
 5. Did resetting the service processor resolve the problem?
 - **Yes: This ends the procedure.**
 - **No:** Contact your next level of support.
 6. If your system uses static IP addressing, add a system manually by performing the following steps:
 - a. From the HMC, select **Server Management**.
 - b. Select **Add Managed System**.
 - c. Select the **Add a managed system** radio button.
 - d. Enter the IP address/Hostname and password.

Does the system appear under system management?

- **Yes: This ends the procedure.**
- **No:** Contact your next level of support.

Resetting the service processor

Use this procedure to reset the service processor.

Note: Use this procedure *only* under the direction of your next level of support or your hardware service provider. During this procedure you will be powering off the system and removing and reapplying AC power.

1. Inform anyone using the server that it will be shut down.
2. Stop all applications that are running on the server.
3. Stop the operating system and server by choosing from the following options:
 - If you have an HMC, shut down all logical partitions and the server. For instructions see Powering off the managed system. Then continue with step 6.
 - If you do *not* have an HMC, continue with the next step.
4. Log in to the system as a user with the authority to run the appropriate shutdown command.
5. At the command line, enter one of the following commands:
 - If your system is running AIX, type `shutdown`
 - If your system is running i5/OS, type `PWRDWN SYS *IMMED`
 - If your system is running Linux, type `shutdown -h now`

These commands stop the operating system. The system power turns off, the power-on light begins to slowly blink, and the system goes into a standby state.

6. Unplug the AC power cord and replug it back in.
7. Start the server. The service processor is reset. **This ends the procedure.**

Resetting the managed system connection from the HMC

Use this procedure to reset the managed system connection from the HMC.

Perform these steps to reset the managed system connection:

1. In the navigation area, open **Server and Partition**.
2. Select **Server Management**.
3. In the contents area, select the server on which you want to reset the connection.
4. Right-click the server and select **Reset or Remove Connection**.
5. Select **Reset Connection**.
6. Click **OK**.

Checking for a duplicate IP address

Use this procedure to check for a duplicate IP address.

Perform these steps to check for a duplicate IP address.

1. On the HMC, right-click the desktop and select **terminal** → **rshterm**.
2. At the terminal, issue this command: `lssyscfg -r sys -F "name,ipaddr"` A list of managed systems' names and their IP address (or host name) will be displayed.
3. Check to see if there are duplicates.

Resetting a 4758 cryptographic battery that has a low battery condition using i5/OS commands

After the 4758 cryptographic battery has been replaced on a system running i5/OS, you will need to write and run an application to reset the battery.

Step 1. Ensure you have the correct firmware level on the cryptographic coprocessor

The application you write will call the Cryptographic_Facility_Control (CSUACFC) verb to reset the low battery condition. However, before the application can be run, the Common Cryptographic Architecture (CCA) firmware level in the cryptographic coprocessor must be at 2.42 or later, and the hex 030B access control point must be enabled in the role used by the application.

Is the i5/OS logical partition running V5R3 or greater?

- **Yes:** The CCA firmware level of the cryptographic coprocessor is already at 2.42 or later. Continue with "Step 2. Verify that the hex 030B access control point is enabled."
- **No:** The i5/OS partition is running V5R2. Ensure that PTF MF31244 is loaded and applied so that the CCA firmware level of the cryptographic coprocessor is at 2.42 or later. Then continue with "Step 2. Verify that the hex 030B access control point is enabled."

Step 2. Verify that the hex 030B access control point is enabled

In order to ensure that the role is able to issue the reset battery command, you need to verify that the hex 030B access control point is enabled. Perform the following steps:

1. Start the ADMIN server using one of the following options:
 - To use an i5/OS™ command line type:
STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
 - To use iSeries Navigator:
 - a. Select **Network** → **Servers** → **TCP/IP** and right-click **HTTP Administration**
 - b. Then click **Start Instance** → **ADMIN**.
2. Access the iSeries Task page Web site at <http://system:2001> (where *system* is the name of the server).

Note: You must log in with a userid that has IOSYSCFG authority in order to perform the steps required in the remainder of this procedure.

3. On the iSeries Tasks page, select **Cryptographic Coprocessor Configuration**.
4. Select **Start secure session**.
5. Select **Manage configuration**.
6. Select **Roles**.
7. Select **Device description** and enter a profile name and pass phrase. The profile name used depends on how the coprocessor was initially configured. Assuming that the Basic configuration wizard (a function within the Cryptographic Coprocessor Configuration utility) was used to configure the coprocessor, the following naming convention were used:
 - If only one profile was created, that profile should be used. The wizard defaults the name to CRYPMSTR for releases prior to V5R4M0 and CRYPSEC1 for V5R4M0. If the name was changed during the configuration, use that name instead.
 - If three profiles were created, the second of the profiles created should be used. The wizard defaults the name to CRYPSEC for releases prior to V5R4M0 and CRYPSEC2 for V5R4M0. If the name was changed during the configuration use the changed name instead.
8. On the Role Management page, select the Default role and click **Display**. Examine the list that is displayed.
9. Choose from the following options:

- If 030B access control point is enabled, click **Done**.
- If the access control is not present in the Default role, modify the Default by performing these steps:
 - a. From the Role Management page, click the Default role and select **Change**.
 - b. Add the 030B access control point to the list of access control points and click **Continue**.

Step 3. Create and run an ILE CL program

To reset the battery low condition, you need to create and run an ILE CL program. Perform the following steps:

1. Create a source physical file using the Create Source Physical File (CRTSRCPF) CL command if a source file is not already available. For example:

```
CRTSRCPF FILE(MYLIB/SRC)
```

2. Create a new member in the file using the Start Source Entry Utility (STRSEU) CL command. For example:

```
STRSEU SRCFILE(MYLIB/SRC) SRCMBR(LOWBAT) TYPE(CLLE)
```

3. Enter the text below into the new member and then save the member and exit.

```
-----
PGM
DCL      VAR(&RETCODE) TYPE(*INT) LEN(4)
DCL      VAR(&RSNCODE) TYPE(*INT) LEN(4)
DCL      VAR(&EXTDTAL) TYPE(*INT) LEN(4) VALUE(0)
DCL      VAR(&EXTDTA) TYPE(*CHAR) LEN(1)
DCL      VAR(&RULECNT) TYPE(*INT) LEN(4) VALUE(1)
DCL      VAR(&RULEARRAY) TYPE(*CHAR) VALUE('RESETBAT')
DCL      VAR(&VERBDTAL) TYPE(*INT) LEN(4) VALUE(0)
DCL      VAR(&VERBDATA) TYPE(*CHAR) LEN(1)

CALLPRC  PRC(CSUACFC) PARM((&RETCODE) +
                           (&RSNCODE) (&EXTDTAL) (&EXTDTA) +
                           (&RULECNT) (&RULEARRAY) (&VERBDTAL) +
                           (&VERBDATA))

ENDPGM
-----
```

4. Compile the module using the Create CL Module (CRTCLMOD) CL Command. For example:

```
CRTCLMOD MODULE(MYLIB/LOWBAT) SRCFILE(MYLIB/SRC)
```

5. Create the program using the Create Program (CRTPGM) CL command specifying BNDSRCPGM(QCCA/CSUACFC). For example:

```
CRTPGM PGM(MYLIB/LOWBAT) MODULE(MYLIB/LOWBAT) BNDSRCPGM(QCCA/CSUACFC)
```

6. Start the program. For example:

```
CALL MYLIB/LOWBAT
```

7. After the reset program has run, vary off and vary on the adapter.


Viewing messages

Learn more about viewing messages to analyze a problem.

When your server detects an error, a message is sent to your console. Where you go to view the message is determined by the operating system that sent the message, and whether you have a Hardware Management Console.

Viewing AIX messages


Learn more about viewing AIX messages.

AIX documentation can be found on the AIX documentation Web site (http://publib16.boulder.ibm.com/pseries/en_US/infocenter/base/aix.htm) .

Viewing HMC messages

Learn more about viewing HMC messages.

For a list of HMC error codes and recovery actions, refer to “HMC error codes” on page 271.

To further troubleshoot a problem, perform maintenance, or install hardware on a Hardware Management Console, see the HMC isolation procedures in the Service provider information .

Viewing IBM i5/OS messages

Learn more about viewing i5/OS messages.

To view i5/OS messages, you can either use the Windows interface in System i Navigator, or a character-based interface on an attached console or emulator session.

Choose the method you want to use:

- View messages with iSeries Navigator
- View messages with a character-based interface

To view messages with System i Navigator:

1. From iSeries Navigator, expand the server with which you want to work.
2. Expand **Basic Operations**.
3. To display messages for the server that you selected, click **Messages**. This displays all the messages for your user profile. Choose from the following options:
 - To reply to, delete, or view the properties for a specific message, right click the message and select the desired action.
 - To send a message, right-click **Messages** and select **Send a message**.
4. To customize your messages view, perform these steps:
 - a. Right-click **Messages**, and select **Customize this View > Include**.
 - b. Expand **Basic Operations**,
 - c. Select **Message queue** and specify the name of the message queue whose messages you want to view. For example, QSYSOPR.
 - d. Specify the name of the library that contains the message queue. If this library is your current library, you can specify **Use current library**. If this library is included in your library list, you can specify **Use library list**.
 - e. Optional: Limit the messages that are displayed by entering a specific numeric value in the **Lowest severity (0–99)** field so that the system displays only the messages that are this severity level or higher.
 - f. Select one or more of the following:
 - Inquiry messages that need a reply
 - Sender’s copy messages that need a reply
 - Messages that do not need a replyTo view all messages in the message queue, select all three.
 - g. Click **OK** to save your changes, and close the Include dialog box.

Refer to the following topics for additional details about i5/OS messages.

- For information about how to display the details or properties of your message, refer to Display message details.
- For information about how to handle potentially severe system messages or messages that require immediate action, refer to the Display messages in the QSYSMSG queue.
- For an overview of i5/OS messages, see Details: Messages.

To view messages with a character-based interface

1. Access the character-based interface.

Note: See Managing the HMC 5250 console for details on accessing a 5250 console session on the HMC.

2. From the command line, enter the Work with Message Queues (WRKMSGQ) command.
3. For more details on using control language (CL) commands, see the CL command finder.

Viewing Linux messages

Learn more about viewing Linux messages.

For Linux messages, refer to the “Reference codes list for customers” on page 263.

Using Service Focal Point

Learn about using the Service Focal Point, an application on the HMC and the Integrated Virtualization Manager, to diagnose and repair problems on the system.

Traditional service strategies become more complicated in a partitioned environment. Each logical partition reports errors it detects, without determining whether other logical partitions also detect and report the errors. For example, if one logical partition reports an error for a shared resource, such as a managed system power supply, other active logical partitions might report the same error. The Service Focal Point application helps you to avoid long lists of repetitive call-home information by recognizing that these are repeated errors and correlating them into one error.

Using Service Focal Point for the HMC

Learn about using the Service Focal Point for the HMC to help you diagnose and repair problems on the system.

Service Focal Point is an application on the HMC that enables you to diagnose and repair problems on the system. In addition, you can use Service Focal Point to initiate service functions on systems and logical partitions that are not associated with a particular problem.

Errors that require service are reported to Service Focal Point as hardware *serviceable events*. The types of hardware serviceable events that are reported include:

- **Call home errors:** These types of errors are automatically reported to IBM service and support.
- **Errors requiring customer intervention:** These types of errors are reported to you by e-mail message and often require you to perform an action to resolve the problem. They do not require assistance from IBM service and support. For example, you might need to clean the tape drive.
- **Errors requiring customer verification:** These types of errors are potentially caused by resources other than IBM resources. These errors require you to verify whether you can solve the problem. If you are unable to solve the problem, you need to manually contact IBM service and support for assistance. For example, if the HMC loses connectivity to the server, you first need to determine if your LAN is causing the problem. If your LAN is down, you need to solve the LAN problem and reconnect the HMC to your server. If the LAN is not causing the problem and you cannot find the source of the problem, contact your next level of support or your hardware service provider.

Note: Software errors are not reported to Service Focal Point.

Viewing serviceable events

Use this procedure to view a serviceable event, including details, comments, and service history.

To view serviceable events and other information about the events, you must be a member of one of the following roles:

- Super administrator
- Service representative
- Operator
- Product engineer
- Viewer

To view serviceable events, follow these steps:

1. In the navigation area, open **Service Applications**.
2. Select **Service Focal Point**.
3. Select **Manage Serviceable Events**.
4. Select the criteria for the serviceable events that you want to view, and click **OK**. The Serviceable Event Overview window opens. The list shows all serviceable events that match your selection criteria. You can use the menu options to perform actions on the serviceable events.
5. Select a line in the Serviceable Event Overview window, and select **Selected** → **View Details**. The Serviceable Event Details window opens, showing detailed information about the serviceable event. The upper table shows information, such as problem number and reference code. The lower table shows the field replaceable units (FRUs) associated with this event.
6. Select the error for which you want to view comments and history, and follow these steps:
 - a. Select **Actions** → **View Comments**.
 - b. When you are finished viewing the comments, click **Close**.
 - c. Select **Actions** → **View Service History**. The Service History window opens, showing service history associated with the selected error.
 - d. When you are finished viewing the service history, click **Close**.
7. When you are finished, click **Cancel** twice to close the Serviceable Event Details window and the Serviceable Event Overview window.

Closing serviceable events

Use this procedure to manually close a serviceable event to remove it from the list of active problems.

In many cases, a serviceable event is closed automatically as part of the repair process. However, if a serviceable event does not require service and no longer requires attention, you can manually close the serviceable event from this interface.

To close a serviceable event, follow these steps:

1. In the navigation area, open **Service Applications**.
2. Select **Service Focal Point**.
3. Select **Manage Serviceable Events**.
4. Select the criteria for the serviceable events that you want to view, and click **OK**. The Serviceable Event Overview window is displayed.
5. Select one or more of the serviceable events that you want to close, and select **Selected** → **Close Event**. The Serviceable Event Comments window opens.
6. Enter comments if necessary, and click **Close Events**.
7. On the Close Serviceable Event dialog, click **Yes** to close the serviceable event.

Viewing serviceable event logical partition information

Use this procedure to view a serviceable event that is related to one of your logical partitions.

When you have a serviceable event related to one of your logical partitions, it is sometimes useful to view information about that problem using Service Focal Point. For example, if you are unable to reproduce the problem because you changed the logical partition configuration after the problem occurred, you can view the logical partition information to see the system configuration at the time of the error and compare it to the current configuration to help you troubleshoot the problem.

1. In the navigation area, open **Service Applications**.
2. Select **Service Focal Point**.
3. Select **Manage Serviceable Events**.
4. Select the criteria for the serviceable events that you want to view, and click **OK**.
5. Select one of the events, and select **Selected** → **Manage Problem Data**.
6. On the Manage Problem Data window, select **Partition Map** and click **View** to see the logical partition information associated with this serviceable event.

Note: The logical partition information pertains to the logical partition configuration at the time the error occurred. Even if you change your logical partition configuration after the error occurred, this information still pertains to the configuration at the time the error occurred.

Repairing serviceable events

Use this procedure to learn how to use the repair process within Service Focal Point to help you exchange a part.

It is often necessary to exchange one or more field replaceable units (FRUs) to repair a serviceable event. For example, you might need to exchange an I/O adapter to solve the problem. You can use the repair process within Service Focal Point to help you exchange the FRU.

To repair a serviceable event, follow these steps:

1. In the navigation area, open **Service Applications**.
2. Select **Service Focal Point**.
3. Select **Repair Serviceable Events**.
4. On the Select Failing System window, select the managed system that has the problem, and click **OK**.
5. Select the serviceable event you want to repair, and select **Selected** → **Repair**. This opens a series of windows that guide you through the steps to repair the serviceable event. The system guides you through one of the two following methods of repair, depending on the type of FRU you need to exchange:
 - An interactive step-by-step process that provides illustrations and video presentations to help you exchange the FRU.
 - A link to the appropriate information center topic that provides instructions to help you exchange the FRU.

After you complete the repair procedure, the system automatically closes the serviceable event.

Activating and deactivating LEDs

Use this procedure to activate or deactivate LEDs using Service Focal Point for the HMC.

Choose from the following:

- “Deactivate a system attention LED or partition LED”
- “Activate or deactivate identify LED” on page 439

Deactivate a system attention LED or partition LED:

You can deactivate a system attention LED or a logical partition LED. For example, you might determine that a problem is not a high priority and decide to repair the problem at a later time. However, you want to be alerted if another problem occurs, so you must deactivate the system attention LED so that it can be activated again if another problem occurs.

1. In the navigation area, open **Service Applications**.
2. Select **Service Focal Point**.
3. Select **Service Utilities**. The Service Utilities window is displayed.
4. Select one of the managed systems, and select **System Attention LED** from the **Selected** menu. The system attention LED window opens. The selected system and its LED state are displayed in the upper part of the window. The logical partition and its LED state are displayed in the lower part of the window. From the system attention LED window, you can deactivate both the system attention LED and the logical partition LED.
5. Select **Deactivate System Attention LED** from the **Action** menu. A confirmation window is displayed that provides the following information:
 - A verification that the system attention LED was deactivated.
 - An indication that there still might be open problems within the system.
 - An indication that you cannot activate the system attention LED.
6. Select one of the logical partitions in the lower table, and select **Deactivate partition LED** from the **Partition Operations** menu. A confirmation window is displayed that provides the following information:
 - A verification that the logical partition LED was deactivated.
 - An indication that there still might be open problems within the logical partition.
 - An indication that you cannot activate the logical partition LED.

Activate or deactivate identify LED:

The system provides several LEDs that help identify various components, such as enclosures or field replaceable units (FRUs), in the system. For this reason, they are called *Identify LEDs*.

You can activate or deactivate the following types of identify LEDs:

- **Identify LED for an enclosure**If you want to add an adapter to a specific drawer (enclosure), you need to know the machine type, model, and serial number (MTMS) of the drawer. To determine whether you have the correct MTMS for the drawer that needs the new adapter, you can activate the LED for a drawer and verify that the MTMS corresponds to the drawer that requires the new adapter.
- **Identify LED for a FRU associated with a specified enclosure**If you want to hook up a cable to a specific I/O adapter, you can activate the LED for the adapter which is a field replaceable unit (FRU), and then physically check to see where you should hook up the cable. This is especially useful when you have several adapters with open ports.

To activate or deactivate an identify LED for an enclosure or FRU, follow these steps:

1. In the navigation area, open **Service Applications**.
2. Select **Service Focal Point**.
3. Select **Service Utilities**. The Service Utilities window is displayed.
4. Select one of the managed systems and select **Selected** → **Identify LED Processing**. The Identify LED, Select Enclosure window opens.
5. To activate or deactivate an identify LED for an enclosure, select an enclosure from the table, and click either **Activate LED** or **Deactivate LED**. The associated LED is either turned on or off.
6. To activate or deactivate an identify LED for a FRU, select an enclosure from the table, select **Selected** → **List FRUs**.
7. Select one or more FRUs from the table, and click either **Activate LED** or **Deactivate LED**. The associated LED is either turned on or off.

Setting up connection monitoring

Use this procedure to set up connection monitoring using Service Focal Point.

Connection monitoring enables you to track the communication paths between your HMC and your managed systems and to create serviceable events when communications problems occur. Use the Service Focal Point application to specify your preferences for connection monitoring. See *Specifying options for connection monitoring* for details on setting up connection monitoring.

Collecting vital product data

Learn how to collect vital product data (VPD) with Service Focal Point for the HMC.

To collect vital product data (VPD), follow these steps:

1. In the navigation area, open **Service Applications**.
2. Select **Service Focal Point**.
3. Select **Collect VPD information**. The Inventory Scout Data Collection window is displayed.
4. Select the managed system that you want to collect data for and click **Next**.
5. Insert a blank, formatted diskette into the floppy drive and click **Finish**.
6. After you are finished, click **Cancel**.

Using Service Focal Point for the Integrated Virtualization Manager

Learn about using the Service Focal Point for the Integrated Virtualization Manager to help you manage problems on your system.

Service Focal Point for the Integrated Virtualization Manager is an application that allows you to manage serviceable events, create serviceable events, manage dumps, and collect vital product data (VPD).

Managing serviceable events with Service Focal Point for the Integrated Virtualization Manager

Learn how to manage serviceable events, including viewing the events' properties, associated FRUs, how to close an event, and how to view additional details.

The padmin user account is not able to run certain serviceable event functions. Users with either the SRUser or DEUser role can run all serviceable event functions.

To view and manage the serviceable events on your managed system, perform the following steps:

1. In the Integrated Virtualization Manager Navigation bar, select **Manage Serviceable Events** (under Service Management).
2. In the Serviceable Event Selection Criteria field, select the criteria for the serviceable events that you want to view, and click **Apply**. The Serviceable Events appear in the table below. The list shows all serviceable events that match your selection criteria. You can use the Tasks options to perform actions on the serviceable events.
3. Choose from the following options:
 - To view properties, continue with step 4.
 - To view associated FRUs, continue with step 5.
 - To close a serviceable event, continue with step 6 on page 441.
 - If you have SRUser role or DEUser role, to view additional details for a serviceable event, continue with step 7 on page 441.
4. To view properties for a serviceable event, select the serviceable event that you want to view properties for and select **Properties**. The Serviceable Event Comments window opens.
5. To view associated field replaceable units (FRUs), select the serviceable event that you want to view FRUs for, and select **View associated FRUs**. The Serviceable Event window opens.

6. To close a serviceable event, select one or more of the serviceable events that you want to close, and select **Close event**. The Serviceable Event Comments window opens.
 - a. Enter comments if necessary, and click **Close Events**.
 - b. On the Close Serviceable Event dialog, click Yes to close the serviceable event.
7. If you have SRUser role or DEUser role, you can view additional details for a serviceable event. Select the serviceable event that you want to view additional details for and select **View additional details**. The Serviceable Event Comments window opens listing additional service objects, each of which has a **Properties** task.

For more information about managing serviceable events, see the online help.

Working with the service utilities on Service Focal Point for the Integrated Virtualization Manager

Learn about the service utilities that are available with the Service Focal Point for the Integrated Virtualization Manager, including how to view or work with errors that are logged against your managed system. Also learn how to invoke service functions on systems and parts that are not associated with a particular problem.

Creating a serviceable event with Service Focal Point for the Integrated Virtualization Manager:

Use this procedure to create a serviceable event on your managed system with the Service Focal Point for the Integrated Virtualization Manager.

You can create a serviceable event to leave a note for yourself or for someone on a later shift to fix or maintain the system.

To create a serviceable event, follow these steps:

1. In the Navigation bar, select **Service Focal Point**.
2. Click **Service Utilities**.
3. In the Service Utilities Menu pane, select **Create Serviceable Event**. The problem description field is displayed.
4. Type the problem description and click **Apply**. A message is displayed stating that the operating completed successfully.

For more information about creating and viewing serviceable events, see the online help.

Managing dumps with Service Focal Point for the Integrated Virtualization Manager:

Use this procedure to manage dumps with Service Focal Point for the Integrated Virtualization Manager.

You can view a list of the system dump files and service processor dumps stored on your managed system. Operating system dump files for individual logical partitions are not included in this list. You also can download dump files to your PC to package and send to service and support for analysis, or you can delete dump files to release storage space on your managed system.

To manage dumps, follow these steps:

1. In the Navigation bar, select **Service Focal Point**.
2. Click **Service Utilities**.
3. In the Service Utilities Menu pane, select **Manage Dumps**. A list of available dumps to manage is displayed.
4. Select the dump you want to work with and click **Delete** or **Download** under the Tasks field.
5. Choose from the following options:

- If you selected Delete, a confirmation window is displayed. Click **OK** to delete the dump. It will be deleted.
- If you selected Download, you will be prompted to save the dump to your system. You can then copy it to a diskette or create a CD to send to service and support.

For more information about managing dump files, see the online help.

Collecting vital product data with Service Focal Point for the Integrated Virtualization Manager

Learn how to collect vital product data (VPD) from the managed system with Service Focal Point for the Integrated Virtualization Manager.

The information in the VPD file can be used to complete the following types of orders for your managed system:

- Install or remove a sales feature
- Upgrade or downgrade a model
- Upgrade or downgrade a feature

To collect vital product data (VPD), follow these steps.

1. In the Service Utilities Menu pane, select **Collect VPD Information**. The Collect VPD Information page is displayed.
2. Click **Collect VPD**. The information is collected, and the VPD file information is displayed.
3. To download the VPD file to your PC, click the link in the VPD File column for the VPD file that you want to download, and follow the prompts to download the file. The VPD file includes the following information about your managed system:
 - Host name
 - Machine type/model
 - Machine serial number
 - Operating system level
 - Feature information
 - Feature location
 - Field Replaceable Unit (FRU)/part number
 - Engineering Change (EC) level
 - Serial number

The VPD information is stored in the `/var/adm/invscout` directory on your hard drive. It is named *hostname.xml* where *hostname* is the name of your host system. For example, *mysystem.xml*.

For more information about collecting vital product data, see the online help.

Replacing and verifying parts

Learn where to find more information about replacing and verifying a customer replaceable unit.

If your troubleshooting leads you to replacing a part that is identified as a customer replaceable unit (CRU), you will need to install the unit and then verify that it is working. To do this, see the Installing features and replacing parts topic.

Reporting problems

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

You can set up your server so that hardware problems are reported electronically. For information about how to set up your service environment, see “Setting up your service environment” on page 31. 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

Learn how you can report problems even if your 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 service and support. 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

Learn what you can do to ensure that hardware problems are reported even if your 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 service and support because this is handled by i5/OS. For more information, see “Setting up IBM i5/OS to connect to service and support without an HMC” on page 77.

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 ASMI, see *Managing the Advanced System Management Interface (ASMI)*. For information about how to set up call-out on your service processor, see “Task 12. Configure the service processor” on page 64.

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

Using the problem reporting forms

Use these forms to collect the information for reporting the problem.

When you discover a problem with the server or logical partition, it might be necessary to report the problem to IBM Support. Refer to the following information to determine how you can collect the appropriate information to provide to IBM Support as they assist you with the problem. Then determine how to contact IBM for service and support.

Problem reporting form for a system in manufacturing default configuration

Use this form to record information about a server in its manufacturing default configuration.

Collect as much of the following information as possible using either the control panel or the Hardware Management Console (HMC) to gather the information.

Note: See Manufacturing default configuration for a description of this configuration.

Required information	Your answers
Your name	
Mailing address	
Telephone number	
Fax number	
IBM customer number, if available	
Date and time that the problem occurred	
Describe the problem	
Machine type	
Model	
Serial number	
Operating system, version, and release	
IPL type	
IPL mode	
Message ID	
Message text	
From/send program	
Instruction number	
To/receive program	
Instruction number	
Service request number (SRN)	SRN: In what mode were AIX diagnostics run? ___ Online or ___ stand-alone ___ Service mode or ___ concurrent mode

Go to the HMC or the control panel and indicate whether the following lights are on:

Control panel light	Place a check if light is on
Power On	
System Attention	

Go to the HMC or control panel to find and record the values for functions 11 through 20. See "Collecting reference codes and system information" on page 260 for step-by-step instructions on collecting reference codes. Use the following grid to record the characters shown on the HMC or Function/Data display.

11	_ _
----	--

Required information	Your answers
IPL type	
IPL mode	
Message ID	
Message text	
From/send program	
Instruction number	
To/receive program	
Instruction number	
Service request number (SRN)	SRN: In what mode were AIX hardware diagnostics run? ___ Online ___ stand-alone ___ Service mode ___ Concurrent mode

Go to the HMC or control panel and indicate whether the following lights are on:

Control panel light	Place a check if light is on
Power On	
System Attention	

Go to the HMC to find and record the values for functions 11 through 20. See “Collecting reference codes and system information” on page 260 for step-by-step instructions on finding reference codes. Use the following grid to record the characters shown on the HMC.

11	<div> <div>— — — — — — — — — —</div> <div>— — — — — — — — — —</div> </div>
12	<div> <div>— — — — — — — — — —</div> <div>— — — — — — — — — —</div> </div>
13	<div> <div>— — — — — — — — — —</div> <div>— — — — — — — — — —</div> </div>
14	<div> <div>— — — — — — — — — —</div> <div>— — — — — — — — — —</div> </div>
15	<div> <div>— — — — — — — — — —</div> <div>— — — — — — — — — —</div> </div>
16	<div> <div>— — — — — — — — — —</div> <div>— — — — — — — — — —</div> </div>
17	<div> <div>— — — — — — — — — —</div> <div>— — — — — — — — — —</div> </div>
18	<div> <div>— — — — — — — — — —</div> <div>— — — — — — — — — —</div> </div>
19	<div> <div>— — — — — — — — — —</div> <div>— — — — — — — — — —</div> </div>
20 (if you use the control panel)	<div> <div>— — — — — — — — — —</div> <div>— — — — — — — — — —</div> </div>

20 (if you use the HMC)	Machine type: Model: Processor feature code: IPL type:
-------------------------	--

Contacting IBM service and support

Use this information to learn how to contact the IBM service and support organization.

In general, the term *service* includes repair of hardware, the ability to ask usage and defect questions about your software, and on-site and remote support for any system concerns through IBM Support.

For up-to-date contact information, visit the Directory of Worldwide Contacts Web site

(www.ibm.com/planetwide/) .

Type of problem	Call
<ul style="list-style-type: none"> • Advice • Migrating • "How to" • Operating • Configuring • Ordering • Performance • General information 	<ul style="list-style-type: none"> • 1-800-IBM-CALL (1-800-426-2255) • 1-800-IBM-4YOU (1-800-426-4968)
Software: <ul style="list-style-type: none"> • Fix information • Operating system problem • IBM application program • Loop, hang, or message Hardware: <ul style="list-style-type: none"> • IBM system hardware broken • Hardware reference code • IBM input/output (I/O) problem • Upgrade 	1-800-IBM-SERV (1-800-426-7378)

Related information for Customer service, support, and troubleshooting

Product manuals, IBM Redbooks® (in PDF format), Web sites, and information center topics contain information related to the Customer service, support, and troubleshooting topic. You can view or print any of the PDF files.

Listed below are sources of information that relate to the Customer troubleshooting and service topic collection.

i5/OS manuals

- Backup and Recovery  (4000 KB)
- Local Device Configuration  (764 KB)

Web sites

- Performing Licensed Internal Code Maintenance module in IBM Resource Link Web site at <http://www.ibm.com/servers/resourcelink>
- AIX documentation Web site at http://publib16.boulder.ibm.com/pseries/en_US/infocenter/base/aix.htm
- Directory of Worldwide Contacts Web site at www.ibm.com/planetwide/
- Electronic Service Agent Web site at <http://www.ibm.com/support/electronic/navpage?category=5>. This Web site enables you to search for the appropriate user's guide for Electronic Service Agent running on AIX or Linux.
- Fix Central Web site at <http://www.ibm.com/eserver/support/fixes/>. This Web site enables you to search for the updates you need for server firmware, HMC machine code, and operating systems.
- POWER5 Code Matrix Web site at <http://www14.software.ibm.com/webapp/set2/sas/f/power5cm/home.html>
- Hardware Management Console Web site at <http://www14.software.ibm.com/webapp/set2/sas/f/hmc/home.html>
- IBM Electronic Services News Web site at <http://www.ibm.com/support/electronic>. Use this Web site to view the server information you have shared with IBM.
- Service and productivity tools for Linux on POWER Web site at <http://www14.software.ibm.com/webapp/set2/sas/f/lopdiags/home.html>
- iSeries Information Center at <http://www.ibm.com/eserver/series/infocenter>. The System i Information Center is a source for technical information about the System i server. The information center is your starting point for all System i technical information.
- Microcode downloads Web site at <http://www14.software.ibm.com/webapp/set2/firmware>.
- My IBM profile Web site at <http://www.ibm.com/account/profile/us>. Use this site to create an IBM ID for each of the people you want to have access to the information that Electronic Service Agent shares with IBM.
- Online Publications Web site at <http://publib.boulder.ibm.com/isrvagt/sdsadoc.html>. This Web site enables you to search for the appropriate simplified activation user's guide for Electronic Service Agent running on i5/OS.
- RFC Editor Web site at <http://www.rfc-editor.org/rfcsearch.html>. This Web site allows you to view RFCs.
- Support for UNIX® servers Web site at <http://www-1.ibm.com/servers/eserver/support/pseries/>
- iSeries integrated xSeries solutions troubleshooting Web site

Other information

- Managing your server and devices
- Cabling the HMC
- Start or stop the system
- Overview of passwords
- Installing features and replacing parts
- **Managing your server using the Advanced System Management Interface:**
 - Initiating a system dump
 - Initiating a service processor dump
- **Managing your server using the Hardware Management Console:**
 - Managing the HMC 5250 console
 - Backing up critical HMC data
 - Accessing the control panel functions using the HMC
 - Disconnecting another HMC connection

- Initializing profile data.
- Resetting the operating system on a logical partition
- Restoring profile data
- Updating managed system or frame information
- Viewing information about the managed system
- Shutting down, rebooting, and logging off the HMC
- Powering off the managed system
- Partitioning the server
 - Creating a system profile
 - Copy a system profile
 - Activating a partition profile
 - Recovering partition data on a managed system
 - Manufacturing default configuration
 - Resetting the server to a nonpartitioned configuration
 - Restarting and shutting down AIX in a logical partition
 - Shutting down i5/OS partitions
 - Restarting and shutting down Linux in a logical partition

Service provider information

- HMC isolation procedures
- (A1xx) Service processor reference (attention) codes
- (A2xx, B2xx) Logical partition reference codes
- (AAxx) Partition firmware reference (attention) codes
- (B3xx) Connection monitoring reference codes
- (BAxx) Partition firmware reference (error) codes
- (CAxx) Partition firmware progress codes
- (C1xx) Service processor progress codes (checkpoints)
- (C2xx) Virtual service processor progress codes
- (C900) i5/OS IPL status progress codes
- (D1xx) Service processor progress codes (service processor dump and platform dump)
- (D1xx) Service processor status progress codes
- General status progress codes (D6xx)
- General status progress codes (D9xx)
- IPL status progress codes
- (C700) Server firmware IPL status progress codes

AIX information AIX documentation can be found on the AIX documentation Web site

(http://publib16.boulder.ibm.com/pseries/en_US/infocenter/base/aix.htm) .

i5/OS information

- CL finder
- Common reference codes for software installation
- Create message queue QSYSMSG for severe messages
- Details: Messages
- Display message details
- Display messages in the QSYSMSG queue

- IPL SRC finder
- Operations Console
- Scenario: Message monitor
- Troubleshoot system reference code (SRC) data for Operations Console
- Use the Analyze Problem (ANZPRB) command
- Use the Work with Problems (WRKPRB) command
- Electronic Service Agent

Appendix. Accessibility features

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use information technology products successfully.

The following list includes the major accessibility features:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are tactilely discernible and do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

IBM and accessibility

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

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
AIX 5L
Electronic Service Agent
eServer
i5/OS
OpenPower
IBM
iSeries
OS/400
POWER
POWER4
POWER5
pSeries
RS/6000
System i5
System p5
Virtualization Engine

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.

Electronic emission notices

Class A Notices

The following Class A statements apply to the IBM System i models and IBM System p servers with the exception of those that are specifically identified as Class B.

Federal Communications Commission (FCC) statement

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

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

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

Industry Canada Compliance Statement

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

Avis de conformité à la réglementation d'Industrie Canada

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

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

European Community contact:
IBM Technical Regulations
Pascalstr. 100, Stuttgart, Germany 70569

Tele: 0049 (0)711 785 1176
Fax: 0049 (0)711 785 1283
E-mail: tjahn@de.ibm.com

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

VCCI Statement - Japan

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス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。

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

This product is a Class A Information Technology Equipment and conforms to the standards set by the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

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

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.

IBM Taiwan Contact Information:

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

Electromagnetic Interference (EMI) Statement - Korea

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이점을 주의하시기 바라며, 만약 잘못 판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Please note that this equipment has obtained EMC registration for commercial use. In the event that it has been mistakenly sold or purchased, please exchange it for equipment certified for home use.

Germany Compliance Statement

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

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

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

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

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

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A.

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

Verantwortlich für die Konformitätserklärung nach des EMVG ist die IBM Deutschland GmbH, 70548 Stuttgart.

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Electromagnetic Interference (EMI) Statement - Russia

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

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

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

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications 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 publications 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 publications 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 THESE PUBLICATIONS. THESE PUBLICATIONS ARE 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.



Printed in USA