ESCALA POWER5

Hardware Information

Managing your server using the Advanced System Management Interface

REFERENCE
86 A1 36EW 00

BLANK

ESCALA POWER5

Hardware Information

Managing your server using the Advanced System Management Interface

Hardware

July 2006

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

REFERENCE
86 A1 36EW 00

Printed in France

Suggestions and criticisms concerning the form, content, and presentation of this book are invited. A form is provided at the end of this book for this purpose.

To order additional copies of this book or other Bull Technical Publications, you are invited to use the Ordering Form also provided at the end of this book.

Trademarks and Acknowledgements

Table of Contents

Managing your server using the Advanced System Management Interface

The Advanced System Management Interface (ASMI) is the interface to the service processor that allows you to set flags that affect the operation of the server, such as auto power restart, and to view information about the server, such as the error log and vital product data.

This interface is accessible using a Web browser on a client system that is connected to the service processor on an Ethernet network. It can also be accessed using a terminal attached to a system port on the server. The service processor and the ASMI are standard on all models and servers models, except for the ESCALA PL 245T/R models. On the ESCALA PL 245T/R models, the SMS menus contain additional options that allow you to perform system management functions, such as powering off or restarting the system and viewing diagnostic data.

On the standard systems, you may be able to use the service processor's default settings. In that case, accessing the ASMI is not necessary.

The following list contains ASMI concepts and tasks that can be performed using the ASMI if you have successfully logged in with the requisite authority level (for additional details, see ASMI authority levels):

- **Printable PDF**
  Print a PDF (Portable Document Format) version of this topic and save it to your workstation.
- **Viewing system information**
  View system power control network (SPCN) trace data, progress indicator history, and vital product data (VPD).
- **Controlling the system power**
  Manually and automatically control the system power.
- **Changing system configuration**
  View and perform custom system configurations, such as enabling PCI (Peripheral Component Interconnect) error injection policies, viewing system identification information, and changing memory configuration.
- **Setting performance options**
  Enhance the performance of your managed system by changing the logical memory block size and enabling cache locking mode.
- **Configuring network services**
  Configure network interfaces, configure network access, and debug the virtual TTY.
- **Using on-demand utilities**
  Activate inactive processors or inactive system memory without restarting your server or interrupting your business.
- **Using concurrent maintenance utilities**
  Replace devices in your server without having to power off your server.
- **Troubleshooting the server using service aids**
  View and customize troubleshooting information with various service aids (such as viewing error logs and initiating service processor dumps).

Printable PDF

Print a PDF (Portable Document Format) version of this topic and save it to your workstation.

To view or download the PDF version of this document, select Managing your server using Advanced System Management Interface (about 250 KB).

You can view or download the related topic Managing the Advanced System Management Interface (about 136 KB).

Saving PDF files

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

1. Right-click the PDF in your browser (right-click the link to the topic).
2. Click Save Target As... if you are using Internet Explorer. Click Save Link As... if you are using Netscape Communicator.
3. Navigate to the directory in which you want to save the PDF file.
4. Click Save.

Downloading Adobe Reader

You need Adobe Reader to view or print these PDFs. You can download a copy from the Adobe Web site .

Parent topic: Managing your server using the Advanced System Management Interface

Viewing system information

View system power control network (SPCN) trace data, progress indicator history, and vital product data (VPD).

This ASMI option provides access to vital product data (VPD) and system power control network (SPCN) trace data.

Attention: Clicking **Back** in the browser might display outdated data. To display the most up-to-date data, select the desired item from the navigation pane.

- **Viewing vital product data**
  View selected or all manufacturer's VPD, such as serial numbers and part numbers.
- **Viewing persistent storage**
  Displays the contents of the registry.
- **Viewing system power control network trace**
  View SPCN trace data that was dumped from the processor subsystem or server drawer.
- **Viewing progress indicator from previous boot**
  Displays the boot progress indicator from the previous system boot.
- **Viewing progress indicator history**
  View progress codes that were shown on the control panel display.
- **Viewing real-time progress indicator**
  Reports the progress codes that currently show on the control panel display.

Parent topic: Managing your server using the Advanced System Management Interface

Viewing vital product data

View selected or all manufacturer's VPD, such as serial numbers and part numbers.

You can view manufacturer's vital product data (VPD) stored from the system boot prior to the one in progress now.

To perform this operation, your authority level must be one of the following:

- General
- Administrator
- Authorized service provider

To view the VPD, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Information and select Vital Product Data.
3. A list of field replaceable units (FRUs) that exist on the system and their descriptions are displayed. Select a single FRU or multiple FRUs from this list that you would like to view.
4. Click Display Details to display the details for selected FRUs, or click Display all details to display details for all VPD entries.

Parent topic: Viewing system information

Viewing persistent storage

Displays the contents of the registry.

You can gather additional debug information from a failing system by viewing the contents of the registry. The term *registry key* can refer to either the key part of a registry entry or the entire registry entry, depending on the context. The registry key hierarchy and the contents of any key can be viewed in both ASCII and hexadecimal formats.

Each registry entry is identified by a two-part key. The first part is the component name, and the second part is the name of the key. For example, the `TerminalSize` key of the esw_menu component is identified as *menu/TerminalSize*. Each registry key also has a value, which is up to 255 bytes of binary data.

To view persistent storage, your authority level must be authorized service provider.

To view the component names of the contents of the registry, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Information and select Persistent Storage.
3. Click the component names to view a list of registry entries.
4. Click the desired registry entry to view the contents of a registry entry.

Parent topic: Viewing system information

Viewing system power control network trace

View SPCN trace data that was dumped from the processor subsystem or server drawer.

You can dump the system power control network (SPCN) trace data from the processor subsystem, or server drawer, to gather additional debug information. Producing a trace may take an extended period of time based on your system type and configuration. This delay is due to the amount of time the system requires to query the data.

Note: Due to the amount of time required to produce a trace, select this option only if it is recommended by an authorized service provider.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To view this trace data, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Information and select System Power Control Network Trace. Trace data is displayed as single contiguous data in two columns.
3. View the raw binary data in the left column and an ASCII translation in the right column.

Parent topic: Viewing system information

Viewing progress indicator from previous boot

Displays the boot progress indicator from the previous system boot.

You can view the progress indicator that displayed in the control panel during the previous failed boot. During a successful boot, the previous progress indicator is cleared. If this option is selected after a successful boot, nothing displays.

To perform this operation, your authority level must be one of the following:

- General
- Administrator
- Authorized service provider

The progress indicator information is stored in nonvolatile memory. If the system is powered off using the power-on button on the control panel, this information is retained. If the ac power is disconnected from the system, this information is lost.

To view the progress indicator from the previous boot, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Information.
3. Select Previous Boot Progress Indicator. The results are displayed in the right pane.

Parent topic: Viewing system information

Viewing progress indicator history

View progress codes that were shown on the control panel display.

You can view progress codes that appeared in the control panel display during the last boot. The codes display in reverse chronological order.

To perform this operation, your authority level must be one of the following:

- General
- Administrator

- Authorized service provider

To view the progress indicator history, perform the following task:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Information.
3. Select Progress Indicator History.
4. Select the desired progress indicator to view additional details and click Show Details. The progress indicator codes are listed from top (latest) to bottom (earliest).

Parent topic: Viewing system information

Viewing real-time progress indicator

Reports the progress codes that currently show on the control panel display.

You can view the progress and error codes that currently display on the control panel. Viewing progress and error codes is useful when diagnosing boot-related issues.

To perform this operation, your authority level must be one of the following:

- General
- Administrator
- Authorized service provider

To view the progress indicator, perform the following task:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Information.
3. Select Real-time Progress Indicator to display a small box that contains the current progress and error codes. If no value is currently on the control panel, the small box is displayed but remains empty.

Parent topic: Viewing system information

Controlling the system power

Manually and automatically control the system power.

This topic provides information on how to use the ASMI to manually and automatically control the system power:

- **Powering the system on and off**
  View and customize various initial program load (IPL) parameters.
- **Setting auto-power restart**
  Enable or disable the function that automatically restarts the system.
- **Performing an immediate power off**
  Power the system off immediately.
- **Performing a system reboot**
  Reboot your system without a complete system shutdown.
- **Setting Wake on LAN**
  Enable or disable the function that powers on a system remotely through a local area network (LAN) connection.

Parent topic: Managing your server using the Advanced System Management Interface

Powering the system on and off

View and customize various initial program load (IPL) parameters.

You can start and shut down the system in addition to setting IPL options.

To perform these operations, your authority level must be one of the following:

- Administrator
- Authorized service provider

Several IPL options that you can set pertain to the server firmware. Firmware is an integral part of the server that is stored in *flash memory*, whose contents are preserved when the system is powered off. The firmware is code that automatically starts when the server is turned on. Its main purpose is to bring the server to a state where it is ready to operate, which means the server is ready to install or boot an operating system. Firmware also enables the handling of exception conditions in the hardware and provides extensions to the functions of the server hardware platform. You can view the server's current firmware level on the Advanced System Management Interface (ASMI) Welcome pane.

This server has a permanent firmware boot side, or P side, and a temporary firmware boot side, or T side. When updating the firmware, install new levels of firmware on the temporary side first to test the compatibility with your applications. When the new level of firmware has been approved, copy it to the permanent side.

To view and change IPL settings, perform the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand Power/Restart Control and select Power On/Off System.
3. Set the following desired boot settings.
   System boot speed
   : Select the speed for the next boot: Fast or Slow. Fast boot results in skipped diagnostic tests and shorter memory tests during the boot.

   Firmware boot side for next boot
   : Select the side from which the firmware boots the next time: Permanent or Temporary. Firmware updates should be tested by booting from the temporary side before being copied into the permanent side.

   System operating mode
   : Select the operating mode: Manual or Normal. Manual mode overrides various automatic power-on functions, such as auto-power restart, and enables the power button.

   AIX/Linux partition mode boot
   : Select the stopping point during the boot process. This option is applicable only to servers servers, and is available only if the system is not managed by the HMC. Service mode boot from saved list is the preferred way to run online AIX diagnostics. Service mode boot from default list is the preferred way to run stand-alone AIX diagnostics.

     This option is applicable only when the managed system is using the manufacturing default configuration, which is the initial partition setup as received from your service provider. When the system is *not* using the manufacturing default configuration, any changes to this option do not take effect. However, when the system *is* using the manufacturing default configuration, you can change the setting for the next restart by changing this option.

   Boot to server firmware
   : Select the state for the server firmware: Standby or Running. When the server is in the server firmware standby state, partitions can be set up and activated.

   System power off policy
   : Select the system power off policy. The system power off policy is a system parameter that controls the system's behavior when the last partition (or the only partition in the case of a system that is not managed by an HMC) is powered off.

   Current hyperboot mode state:
   : This setting appears if the hyperboot feature is activated for the system. The hyperboot mode states are: `capable` and `enabled`. When the hyperboot feature is activated by entering the activation code, the mode state initializes in the ASMI and displays *capable* until the system is restarted. After the system has restarted the state changes to *enabled*. Any time you restart the system in the enabled state, it starts in hyperboot mode.

Note: This setting can not be changed by using this task. See Using on-demand utilities for information about entering a feature activation code to enable this feature.

4. Perform one of the following steps:
   - 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 available only 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. This option is available only if the server firmware is in *standby* mode.

Parent topic: Controlling the system power

Setting auto-power restart

Enable or disable the function that automatically restarts the system.

You can set your system to automatically restart. This function is useful when power has been restored and any backup power supply has recharged after a temporary power failure or after an unexpected power line disturbance that caused the system to shut down unexpectedly. Auto-power restart will only work if the "system operating mode" is set to *normal* in the Power On/Off System settings. For information about setting the system operating mode, see Powering the system on and off.

When the system restarts, it returns to the state it was in at the time of the power loss. If the system is not managed by a Hardware Management Console (HMC), the system reboots the operating system. If the system is managed by an HMC, all of the partitions that were running before the power loss are reactivated.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To set the auto-power restart function, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand Power/Restart Control and select Auto Power Restart.
3. Select either Enable or Disable from the selection list. By default, the state for auto-power restart is *Disable*.
4. Click Save settings to save the selected options.

Parent topic: Controlling the system power

Performing an immediate power off

Power the system off immediately.

You can power off your system faster by using the immediate power off option. Typically, this option is used when an emergency power off is needed. The operating system is *not* notified before the system is powered off.

Attention: To avoid experiencing data loss and a longer IPL the next time the system or logical partitions are booted, shut down the operating system prior to performing an immediate power off.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To perform an immediate power off, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand Power/Restart Control and select Immediate Power Off.
3. Click Continue to perform the operation.

Parent topic: Controlling the system power

Performing a system reboot

Reboot your system without a complete system shutdown.

You can reboot the system.

Attention: Rebooting the system immediately shuts down all partitions.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To perform a system reboot, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand Power/Restart Control and select System Reboot.
3. Click Continue to perform the operation.

Parent topic: Controlling the system power

Setting Wake on LAN

Enable or disable the function that powers on a system remotely through a local area network (LAN) connection.

You can power on a system remotely through a local area network (LAN) connection. Wake on LAN can be enabled for logical partition configurations, as well as nonpartitioned environments.

Note: Wake on LAN is supported on Ethernet port 0. It is not supported on Ethernet port 1. On model server, use port Un-P1-T5 to enable Wake on LAN. It is not supported on models ESCALA PL 3250R, and ESCALA PL 6450R.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To enable or disable Wake on LAN, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand Power/Restart Control and select Wake On LAN.
3. Select either Enable or Disable from the selection list. By default, the state for Wake on LAN is *Disable*.
4. Click Save settings to save the selected options.

Parent topic: Controlling the system power

Changing system configuration

View and perform custom system configurations, such as enabling PCI (Peripheral Component Interconnect) error injection policies, viewing system identification information, and changing memory configuration.

This topic provides instructions that should be used to view and perform custom system configurations:

- **Changing system name**
  Change the name of the system.
- **Changing the processing unit identifier**
  Change the processing unit ID, also referred to as the processing unit system power control network (SPCN) ID.
- **Configuring I/O enclosures**
  View and change various enclosure attributes.
- **Changing the time of day**
  Display and change the time and date stored by the system.
- **Changing firmware update policy**
  Configure your system to only allow firmware updates from the selected source.
- **Enabling PCI error injection policy**
  Change the PCI error injection policy that forces errors to be injected to PCI cards.
- **Configuring monitoring**
  Configure the server firmware, HMC, and service processor connection monitoring.
- **Disconnecting an HMC**
  Display and disconnect HMCs connected to the managed system.
- **Changing the interposer plug count**
  View and change the multiple chip module (MCM) interposer plug count.
- **Changing the number of HSL Opticonnect Connections**
  View and change the maximum number of Highspeed Link (HSL) Opticonnect Connections allowed for your system.
- **Enabling I/O adapter memory allocation**
  Increase the amount of PCI memory space allocated to specified PCI slots.
- **Deconfiguring hardware**
  Set deconfiguration policies, change processor configuration, change memory configuration, and clear all deconfiguration errors.
- **Configuring virtual Ethernet environment settings**
  Specify settings to control your virtual Ethernet environment.
- **Programming vital product data**
  Program vital product data (VPD) such as system brand, system identifiers, and system enclosure type.
- **Changing service indicators**
  Turn off system attention indicator, enable enclosure indicators, change indicators by location code,

and perform an LED test on the control panel.

Parent topic: Managing your server using the Advanced System Management Interface

Changing system name

Change the name of the system.

You can change the name that is used to identify the system. This name helps your support team (for example, your system administrator, network administrator, or authorized service provider) to more quickly identify the location, configuration, and history of your server.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

The system name is initialized to the 31-character value `Server-tttt-mmm-SNoooooo`, where the substitution characters mean the following:

Characters	Description
tttt	Machine type
mmm	Model number
ooooooo	Serial number

The system name can be changed to any valid ASCII string. It does not have to follow the initialized format.

To change the system name, do the following:

1. In the navigation area, expand System Configuration.
2. Select System Name.
3. Enter the desired system name using the previous naming convention.
4. Click Save settings to update the system name to the new value.

The new system name is displayed in the status frame, the area where the logout button is located. If another method, such as the HMC, is used to change the system name, the status frame does not reflect the change.

Parent topic: Changing system configuration

Changing the processing unit identifier

Change the processing unit ID, also referred to as the processing unit system power control network (SPCN) ID.

Use this task if you need to change the processing unit identifier (SPCN ID). The processing unit SPCN ID is used by the SPCN firmware to identify the system type. It is also used to identify the primary service processor if there are two service processors in the system.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

Note: This feature is available only when the system is powered off. This operation resets the service processor.

To change the processing unit identifier, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Configuration.
3. Select Processing Unit Identifier.
4. Enter the desired information into the 2-character text area. Supported processing unit identifiers are shown in the following table:

Model or expansion unit	**Processing unit identifier**
7/10	BA
112/85	B4
7/20	BB
ESCALA PL 250R-VL or ESCALA PL 450R-XS	C0
ESCALA PL 250R-L and ESCALA PL 250R-L+ or ESCALA PL 450R-VL+	BA
ESCALA PL 250T/R and ESCALA PL 250T/R+ or ESCALA PL 450T/R-L+	B4
ESCALA PL 450T/R and ESCALA PL 450T/R+ or ESCALA PL 850T/R-L+	B5
ESCALA PL 1650R-L+	B2
ESCALA PL 850R/PL 1650R/R+	B2
ESCALA PL 850R/PL 1650R/R+ (with one or more secondary units)	B3
5/75	B9
ESCALA PL 3250R and ESCALA PL 6450R	B1
50/74 and 50/79	81
50/88 and 05/88	89
50/94 and 52/94	8A
05/95 and 50/95	8B
57/90	88
11D/10	88
11D/11	88
11D/20	8C

Note: Processing unit IDs are not applicable f, ESCALA PL 245T/R, and the D24 and T24 enclosure models.

5. Click Save settings to complete the operation.

Parent topic: Changing system configuration

Configuring I/O enclosures

View and change various enclosure attributes.

After the server firmware has reached the *standby* state, you can configure I/O enclosure attributes as follows:

- List the status, location code, rack address, unit address, power control network identifier, and the machine type and model of each enclosure in the system.
- Change the identification indicator state on each enclosure to *identify* or *off*.
- Update the power control network identifier, enclosure serial number, and the machine type and model of each enclosure.
- Change the identification indicator state of the SPCN firmware in a enclosure to *Enable* or *Disable*.
- Remove rack and unit addresses for all inactive enclosures in the system.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To configure I/O enclosures, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Configuration and select Configure I/O Enclosures.
3. Select the enclosure and the desired operation. If you select Change settings, click Save setting to complete the operation.

Parent topic: Changing system configuration

Changing the time of day

Display and change the time and date stored by the system.

You can display and change the system's current date and time. The date and time can only be changed when the system is powered off. The time is stored as UTC (Coordinated Universal Time), formerly expressed as Greenwich mean time (GMT).

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

Note: You can change the time of day only when the system is powered off.

To change the time of day, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Configuration.

3. Select Time of Day. If the system is powered off, the right pane displays a form that shows the current date (month, day, and year) and time (hours, minutes, seconds).
4. Change either the date value or the time value or both, and click Update Time Of Day.

Parent topic: Changing system configuration

Changing firmware update policy

Configure your system to only allow firmware updates from the selected source.

Note: These options are only valid if your server is managed by an HMC, otherwise the default source for installing firmware updates is the operating system and setting the source using this method is ignored by the server.

You can change the source for firmware updates. For example, if you choose the Hardware Management Console (HMC) as the source for a firmware update, the HMC must be used to perform the update. The HMC performs all tasks to update the server firmware.

Parent topic: Changing system configuration

Updating firmware on servers

If your server has an HMC attached, the firmware update can only be performed from the HMC. The firmware update must be initiated from the HMC concurrently (while the system is running), but the update will not be applied until the server is rebooted. If your server does not have an HMC attached, the firmware update must be performed from the operating system. The system reboots immediately to apply the update.

Firmware updates for servers are available on the Web. For more information, see Getting fixes in the Service and support topic.

Enabling PCI error injection policy

Change the PCI error injection policy that forces errors to be injected to PCI cards.

You can enable or disable the injection of errors on the PCI bus. For example, independent software vendors who develop device drivers can inject errors to test the error handling code in the device driver.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

Note: To inject errors, you will need special hardware in addition to having advanced PCI bus knowledge.

To enable or disable the PCI error injection policy, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Configuration.
3. Select PCI Error Injection Policy.
4. In the right pane, select Enabled or Disabled.
5. Click Save settings.

Parent topic: Changing system configuration

Configuring monitoring

Configure the server firmware, HMC, and service processor connection monitoring.

You can configure your service processor to monitor the system and the system to monitor the service processor. By enabling the various monitoring options, the service processor can ensure that critical system components are functioning while the system is in the *Power off*, *IPL*, and *Running* states.

To configure monitoring, your authority level must be an authorized service provider.

Monitoring is accomplished by periodic samplings called *heartbeats*, which can detect a service processor, HMC, or server firmware connection failure. For example, if the service processor connection monitoring is enabled, each service processor monitors redundant service processor communication to keep track of the status of the other service processor. When the service processor detects no heartbeat from the other service processor, the heartbeat-initiating service processor logs an error due to this communication failure. If this condition persists, the service processor leaves the machine powered on, logs an error, and performs recovery.

To configure monitoring, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Configuration.
3. Select Monitoring.
4. Select Enabled or Disabled for the server firmware, service processor connection monitoring, and HMC. All connection monitoring fields are enabled by default.
5. Click Save settings. Monitoring does not take effect until the next time the operating system is started.

Parent topic: Changing system configuration

Disconnecting an HMC

Display and disconnect HMCs connected to the managed system.

You can display and disconnect HMCs connected to the managed system. By default, HMC connection data expires on the managed system after 14 days of disconnection from the HMC. If you want to perform a task that requires all HMCs to be disconnected from the managed system, you can remove the HMC connection data prior to the 14-day period.

To disconnect an HMC, your authority level must be an authorized service provider.

To disconnect an HMC, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Configuration.
3. Select HMC Connections.
4. Select the desired HMC.
5. Click Save settings.

Parent topic: Changing system configuration

Changing the interposer plug count

View and change the multiple chip module (MCM) interposer plug count.

You can track the number of times that a multiple chip module (MCM) has been replaced or reseated on a given interposer. This interposer plug count provides you with information needed to prevent field problems due to damaged or overused interposers. You can use the ASMI to view and alter the interposer plug count for all MCMs in the system. Whenever a service action is performed on a system that requires the replacement or reseating of an MCM, service personnel are responsible for updating the plug count for that interposer.

Note: The Interposer Plug Count option is supported only on certain system types and models. If your server does not support this option and you select this option from the menu, the firmware returns a message indicating that this option is not applicable to your system.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To view and modify the interposer plug count, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Configuration.
3. Select Interposer Plug Count. The current plug count is displayed in the text edit field for each MCM interposer. Each interposer is identified by location code.
4. Type a new value into the text field to change the plug count.
5. Click Save settings. A report page displays the new value.

Parent topic: Changing system configuration

Changing the number of HSL Opticonnect Connections

View and change the maximum number of Highspeed Link (HSL) Opticonnect Connections allowed for your system.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To change the number of HSL Opticonnect Connections, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Configuration.
3. Select HSL Opticonnect Connections. The current number of HSL Opticonnect Connections for the system is displayed.
4. Type a new value into the Custom text field, or to permit the system to automatically determine the maximum number of HSL Opticonnect Connections allowed for the system, select Automatic.
5. Click Save settings.

Parent topic: Changing system configuration

Enabling I/O adapter memory allocation

Increase the amount of PCI memory space allocated to specified PCI slots.

You can increase the amount of I/O adapter memory for specified PCI slots. When the I/O Adapter Enlarged Capacity option is enabled, specific PCI slots receive the largest memory-mapped address spaces that are available.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To enable or disable I/O adapter memory allocation, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Configuration.
3. Select I/O Adapter Enlarged Capacity.
4. In the right pane, select Enabled or Disabled.
5. Click Save settings.

Parent topic: Changing system configuration

Deconfiguring hardware

Set deconfiguration policies, change processor configuration, change memory configuration, and clear all deconfiguration errors.

- **Setting deconfiguration policies**
  Set various processor and memory configuration and deconfiguration policies.
- **Changing processor configuration**
  Display data for each processor. You can change the state of each processor.
- **Changing memory configuration**
  Display data for each memory unit (DIMM) and bank. You can change the state of each bank.
- **Manually deconfiguring a processing unit**
  View deconfiguration information and manually deconfigure a processing unit (node).
- **Clearing all deconfiguration errors**
  Clear error records for specific or all resources in the system.

Parent topic: Changing system configuration

Setting deconfiguration policies

Set various processor and memory configuration and deconfiguration policies.

You can set various policies to deconfigure processors and memory in certain situations. You can enable policies that will deconfigure the processor when failures occur, such as a predictive failure (for example, correctable errors generated by a processor exceeding the threshold), floating point failure, functional failure, or system bus failure. You can also enable the firmware to power off a processing unit (node) for concurrent maintenance when any of the resources in that node are deconfigured.

To set the deconfiguration policies, your authority level must be one of the following (any user can view the deconfiguration policies):

- Administrator
- Authorized service provider

To set deconfiguration policies, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Configuration and Hardware Deconfiguration.
3. Select Deconfiguration Policies.
4. In the right pane, select Enabled or Disabled for each policy.
5. Click Save settings.

Parent topic: Deconfiguring hardware

Changing processor configuration

Display data for each processor. You can change the state of each processor.

All processor failures that stop the system, even if intermittent, are reported to the authorized service provider as a diagnostic call out for service repair. To prevent the recurrence of intermittent problems and improve the availability of the system until a scheduled maintenance window, processors with a failure history are marked *deconfigured* to prevent them from being configured on subsequent boots.

A processor is marked *deconfigured* under the following circumstances:

- A processor fails a built-in self-test or power-on self-test testing during boot (as determined by the service processor).
- A processor causes a machine check or check stop during run time, and the failure can be isolated specifically to that processor (as determined by the processor run-time diagnostics in the service processor firmware).
- A processor reaches a threshold of recovered failures that results in a predictive call to service (as determined by the processor run-time diagnostics in the service processor firmware).

During system start time, the service processor does not configure processors that are marked *deconfigured*. The deconfigured processors are omitted from the hardware configuration. The processor remains offline for subsequent reboots until it is replaced or the deconfiguration policy is disabled. The deconfiguration policy also provides the user with the option of manually deconfiguring a processor or re-enabling a previously manually-deconfigured processor. This state is displayed as *deconfigured by user*.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

Note: The state of the processor can be changed only if the system is powered off. At run time, users can view but not change the state of each processor. If the deconfiguration policy is disabled, the states of the processors cannot be changed.

To view or change the processor configuration, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Configuration and Hardware Deconfiguration.
3. Select Processor Deconfiguration.
4. In the right pane, select a node from the list of nodes displayed.
5. Click Continue to change the state of each processor to configured, or deconfigured if it is not already deconfigured by the system.
6. Reboot the system for the changes to take effect.

Parent topic: Deconfiguring hardware

Changing memory configuration

Display data for each memory unit (DIMM) and bank. You can change the state of each bank.

Each memory bank contains two DIMMs (dual inline memory module). If the firmware detects a failure, or predictive failure, of a DIMM, it deconfigures the DIMM with the failure, as well as the other DIMM, in the memory bank. If memory DIMMs are being monitored for errors, each memory bank will be in one of the following states:

- Configured by system (cs)
- Manually configured (mc)
- Deconfigured by system (ds)
- Manually deconfigured (md)

With ASMI you can change the state of the memory bank from *cs* to *md*, from *mc* to *md*, and from *md* to *mc* for one or more DIMMs. If one DIMM is deconfigured, the other DIMM in the memory bank automatically becomes deconfigured.

Note: You can change the state of the memory bank only if the deconfiguration policy is enabled for the memory domain. If this policy is not enabled and you try to change the state, an error message is displayed.

The error type is the cause of memory deconfiguration and applies to the bank in the *ds* state. The error type is displayed only when the bank is in the *ds* state.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To view or change the memory configuration, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Configuration and Hardware Deconfiguration.
3. Select Memory Deconfiguration.
4. In the right pane, select a node from the list of nodes displayed.

5. Click Continue to change the state of memory to configured or deconfigured, if it is not already deconfigured by the system.

   Note: The state of the memory can be changed only if the system is powered off. At run time, users can view, but not change, the state of each processor. If the deconfiguration policy function is disabled, the state of the memory cannot be changed.

6. Click Submit. A report page is displayed, which indicates success or failure when the state of the memory bank has been changed.

Parent topic: Deconfiguring hardware

Manually deconfiguring a processing unit

View deconfiguration information and manually deconfigure a processing unit (node).

You can view the current deconfiguration state for the processing units (nodes) in your network environment. The Advanced System Management interface displays the current configuration state and error-type for processing units in the deconfiguration state. You can also take a processing unit offline by manually deconfiguring the unit. The processing unit must be in the standby state before you can manually deconfigure it.

To manually deconfigure a processing unit, your authority level must be one of the following:

- Administrator
- Authorized service provider

To manually deconfigure a processing unit, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Configuration > Hardware Deconfiguration.
3. Select Processing Unit Deconfiguration.
4. In the right pane, for the node that you want to deconfigure, change the settings from Configured to Deconfigured.
5. Click Save settings. After you manually deconfigure a processing unit, the ASMI displays the configuration state as *deconfigured by user*.

Parent topic: Deconfiguring hardware

Clearing all deconfiguration errors

Clear error records for specific or all resources in the system.

The ASMI allows you to clear error records for all or individual system hardware resources that include the processor, memory, L2 and L3 cache, I/O hubs, service processor card, and clock card.

To clear all deconfiguration errors, your authority level must be an authorized service provider.

Note: Before performing this operation, record error messages or ensure that the error record data is no longer needed; otherwise, you will lose all error data from the hardware resources.

To clear all deconfiguration errors, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Configuration and Hardware Deconfiguration.
3. Select Clear All Deconfiguration Errors.
4. In the right pane, select the desired hardware resource from the drop-down menu. You may select All hardware resources or an individual resource.
5. Click Clear errors for selected hardware resource.

Parent topic: Deconfiguring hardware

Configuring virtual Ethernet environment settings

Specify settings to control your virtual Ethernet environment.

You can configure system firmware settings that enable you to restrict virtual input/output connectivity between partitions and control the number of virtual Ethernet switches allocated by the firmware. The following topics describe these tasks:

- **Managing virtual I/O connectivity**
  Use the ASMI to set the policy for virtual input/output connectivity.
- **Setting the maximum number of virtual Ethernet switches**
  Control the number of virtual Ethernet switches allocated by the system server firmware.

Parent topic: Changing system configuration

Managing virtual I/O connectivity

Use the ASMI to set the policy for virtual input/output connectivity.

Specifying this configuration setting enables you to control virtual input/output activity between partitions. The policy is set to *enabled* by default, which allows all virtual input/output connectivity between partitions. If this setting is disabled, only virtual TTY sessions to the Hardware Management Console (HMC) are allowed.

To set the policy for virtual I/O connections, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log in.
2. In the navigation area, expand System Configuration, and then click Virtual I/O Connections.
3. Select either enable or disable to change the setting.
4. Click Save Settings.

Parent topic: Configuring virtual Ethernet environment settings

Setting the maximum number of virtual Ethernet switches

Control the number of virtual Ethernet switches allocated by the system server firmware.

You can set a configuration value that enables you to specify the number of virtual Ethernet switches that can be allocated by the system server firmware. This value is set to 0 by default. A value of 0 enables the

Hardware Management Console (HMC) to control the number of virtual Ethernet switches allocated by the system server firmware. You can change this value to specify up to 16 allowable virtual switches.

The default value is generally recommended for most configurations. However, in a more complex environment where you might want the system server firmware to create a larger number of virtual Ethernet switches during platform power-on, you can set this number higher and override the HMC's control.

After setting this value, when a virtual Ethernet adapter is created using the HMC, the adapter will be connected to a particular virtual switch depending on the virtual slot number chosen during creation. The adapter's virtual slot number will be divided by the number of virtual Ethernet switches, and the remainder of this division operation will be used to determine with which switch the adapter will be associated. Each virtual Ethernet adapter will only be able to communicate with other virtual Ethernet adapters on the same virtual switch.

To configure the value for virtual Ethernet switches, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log in.
2. In the navigation area, expand System Configuration, and then click Virtual Ethernet Switches.
3. Enter a value for the Number of Virtual Ethernet Switches. The value can be a whole number from 0 to 16.
4. Click Save Settings to save the configuration.

For example, if you set the number of virtual Ethernet switches to 3, virtual Ethernet adapters in virtual slot 3, 6, and 9 are assigned to the same switch. A virtual Ethernet adapter in virtual slot 4 would be assigned to another switch, and would not be able to communicate with the adapters in slots 3, 6, and 9.

Parent topic: Configuring virtual Ethernet environment settings

Programming vital product data

Program vital product data (VPD) such as system brand, system identifiers, and system enclosure type.

The ASMI allows you to program the system vital product data (VPD). To access any of the VPD-related panels, your authority level must be administrator or authorized service provider.

Note: You cannot boot the system until valid values are entered for the system brand, system identifiers, and system enclosure type.

- **Setting the system brand**
  Set and view the system brand.
- **Setting the system identifiers**
  Set the system-unique ID, system serial number, machine type, and machine model.
- **Setting the system enclosure type**
  Set values that uniquely identify the type of enclosures attached to the system.

Parent topic: Changing system configuration

Setting the system brand

Set and view the system brand.

The system brand identifies your system using a 2-character system brand.

Changing the system brand is only allowed if the value has not been set, or if the current value is P0 and the new value will be D0.

Note: You cannot boot the system until valid values are entered for all fields. Use this procedure only under the direction of your service provider.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To change the system brand, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Configuration and Program Vital Product Data.
3. Select System Brand. In the right pane, the current system brand is displayed. If the system brand has not been set, you will be prompted to enter the system brand. Enter the values as specified by your service provider.
4. Click Continue. Your system brand setting and the following notice are displayed:

   ```
   Attention: Once set, this value cannot be changed unless it is 'P0', and
   then only to 'D0'.
   ```
5. Click Save settings to update the system brand and save it to the VPD.

Parent topic: Programming vital product data

Setting the system identifiers

Set the system-unique ID, system serial number, machine type, and machine model.

You can set the system-unique ID, serial number, machine type, and machine model. If you do not know the system-unique ID, contact your next level of support.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

Note: You cannot boot the system until valid values are entered for all fields. You can change these entries only once.

To set the system keywords, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Configuration and Program Vital Product Data.
3. Select System Keywords.
4. In the right pane, enter the desired values for the system serial number, machine type, and machine model using the naming convention shown in the ASMI help. Set the Reserved field to blank spaces unless directed otherwise by service and support.
5. Click Continue. The data validation panel is displayed, which includes your entered settings.
6. Click Save settings to update the system keywords and save them to the VPD.

Parent topic: Programming vital product data

Setting the system enclosure type

Set values that uniquely identify the type of enclosures attached to the system.

When setting the system enclosure type, ensure that the enclosure serial number field matches the original value, which can be found on a label affixed to the unit. Updating the enclosure serial field keeps the configuration and error information synchronized, and this information is used by the system when creating the location codes. This task must be done using the ASMI, not with the control panel. However, if you do not have access to the ASMI, the system will still operate without updating this information.

For example, when replacing the I/O backplane, you must re-enter the original enclosure serial number into the enclosure serial number field to overwrite the serial number that is recorded for the new I/O backplane. Failure to enter the correct enclosure serial number will result in logical partition mappings being incorrect.

Note: You cannot boot the system until valid values are entered for all fields in the enclosure-type information.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To change the system enclosure type, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Configuration > Program Vital Product Data.
3. Select System Enclosures. In the right pane, the current system enclosures are displayed.
4. Enter the desired settings for the Enclosure location, Feature Code/Sequence Number, and Enclosure serial number fields using the naming convention described in the ASMI help.

   The value of the Enclosure serial number field is different than the serial number of the system. Set the Reserved field to blank spaces unless directed otherwise by Level 3 technical support.
5. Click Save settings to update the system enclosure type information and save it to the VPD.

Parent topic: Programming vital product data

Changing service indicators

Turn off system attention indicator, enable enclosure indicators, change indicators by location code, and perform an LED test on the control panel.

The service indicators alert you that the system requires attention or service. It also provides a method for identifying a field-replaceable unit (FRU) or a specific enclosure within the system.

A hierarchical relationship exists between FRU indicators and enclosure indicators. If any FRU indicator is in an *identify* state, then the corresponding enclosure indicator will change to an *identify* state automatically. You cannot turn off the enclosure indicator until all FRU indicators within that enclosure are in an *off* state.

- **Turning off system attention indicator**
  Read about the system attention indicator and how to turn it off.
- **Enabling enclosure indicators**
  Find out how to display and change FRU indicators within each enclosure.
- **Changing indicators by location code**
  Enter FRU indicator location code to set its LED to the *identify* or *off* state.
- **Performing an LED test on the control panel**
  Perform an LED test on the control panel.

Parent topic: Changing system configuration

Turning off system attention indicator

Read about the system attention indicator and how to turn it off.

The system attention indicator provides a visual signal that the system as a whole requires attention or service. Each system has a single system attention indicator. When an event occurs that either needs your intervention or service, the system attention indicator lights continuously. The system attention indicator is turned on when an entry is made in the service processor error log. The error entry is transmitted to the system level and operating system error logs.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To turn off the system attention indicator, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Configuration and Service Indicators.
3. Select System Attention Indicator.
4. In the right pane, click Turn off system attention indicator. If the attempt is unsuccessful, an error message is displayed.

Parent topic: Changing service indicators

Enabling enclosure indicators

Find out how to display and change FRU indicators within each enclosure.

You can turn on or off the *identify* indicators in each enclosure. An *enclosure* is a group of indicators. For example, a processing unit enclosure represents all of the indicators within the processing unit and an I/O enclosure represents all of the indicators within that I/O enclosure. Enclosures are listed by their location code.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To enable the enclosure indicator states, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Configuration and Service Indicators.
3. Select Enclosure Indicators.
4. Select the enclosure of choice and click Continue.
5. Make the necessary changes to the selection list located next to each location code.
6. To save the changes made to the state of one or more FRU indicators, click Save settings.

   To turn off all of the indicators for this enclosure, click Turn off all. A report page is displayed indicating success or failure.

Parent topic: Changing service indicators

Changing indicators by location code

Enter FRU indicator location code to set its LED to the *identify* or *off* state.

You can specify the location code of any indicator to view or modify its current state. If you provide the wrong location code, the advanced system manager attempts to go to the next higher level of the location code.

The next level is the base-level location code for that field replaceable unit (FRU). For example, a user types the location code for the FRU located on the second I/O slot of the third enclosure in the system. If the location code for the second I/O slot is incorrect (the FRU does not exist at this location), an attempt to set the indicator for the third enclosure is initiated. This process continues until a FRU is located or no other level is available.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To change the current state of an indicator, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Configuration and Service Indicators.
3. Select Indicators by Location code.
4. In the right pane, enter the location code of the FRU and click Continue.
5. Select the preferred state from the list.
6. Click Save settings.

Parent topic: Changing service indicators

Performing an LED test on the control panel

Perform an LED test on the control panel.

You can perform an LED test on the control panel to determine if one of the LEDs is not functioning properly.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To perform an LED test on the control panel, perform the following task:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Configuration and Service Indicators.
3. Select Lamp Test.
4. On the Lamp Test pane, click Continue to perform the lamp test. The test changes all indicators to the *identify* state for a short time (approximately 4 minutes).

Parent topic: Changing service indicators

Setting performance options

Enhance the performance of your managed system by changing the logical memory block size and enabling cache locking mode.

This information describes how to enhance the performance of your managed system.

- **Changing the logical memory block size**
  Enhance the managed system performance by manually or automatically changing the logical memory block size.
- **Enabling cache locking mode**
  Improve your system performance by enabling cache locking mode.

Parent topic: Managing your server using the Advanced System Management Interface

Changing the logical memory block size

Enhance the managed system performance by manually or automatically changing the logical memory block size.

The system kernel uses the memory block size to read and write files. By default, the logical memory block size is set to Automatic. This setting allows the system to set the logical block memory size based on the physical memory available. You can also manually change the logical memory block size.

To select a reasonable logical block size for your system, consider both the performance desired and the physical memory size. Use the following guidelines when selecting logical block sizes:

- On systems with a small amount of memory installed (2 GB or less), a large logical memory block size results in the firmware consuming an excessive amount of memory. Firmware must consume at least 1 logical memory block. As a general rule, select the logical memory block size to be no greater than 1/8th the size of the system's physical memory.
- On systems with a large amount of memory installed, small logical memory block sizes result in a large number of logical memory blocks. Because each logical memory block must be managed during boot, a large number of logical memory blocks can cause boot performance problems. It is recommended to limit the number of logical memory blocks to 8 K or less.

Note: The logical memory block size can be changed at run time, but the change does not take effect until the system is restarted.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To configure logical memory block size, perform the following task:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand Performance Setup.
3. Select Logical Memory Block Size.
4. In the right pane, select the logical memory block size and click Save settings.

Parent topic: Setting performance options

Enabling cache locking mode

Improve your system performance by enabling cache locking mode.

You can improve your system performance by enabling the cache locking mode. Performance improvements vary depending on the applications running on your system. It is recommended that you change this setting only if advised by your service provider.

To perform this operation, your authority level must be authorized service provider.

To enable or disable cache locking mode, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand Performance Setup.
3. Select Cache Locking Mode.
4. In the right pane, select Enabled or Disabled.
5. Click Save settings.

Parent topic: Setting performance options

Configuring network services

Configure network interfaces, configure network access, and debug the virtual TTY.

This information describes how to use the ASMI to view and configure network settings:

- **Configuring network interfaces**
  Configure the number and type of network interfaces according to the needs of your system.
- **Configuring network access**
  Specify which IP addresses will be allowed to access the server.
- **Using extended services**
  Specify the IP address and directory path for remote systems.
- **Debugging virtual TTY**
  Debug virtual TTY from the master service processor.

Parent topic: Managing your server using the Advanced System Management Interface

Configuring network interfaces

Configure the number and type of network interfaces according to the needs of your system.

You can configure network interfaces on the system. The number and type of interfaces vary according to the specific needs of your system.

Attention: This operation can be performed when the system is powered on as well as powered off. Because network configuration changes occur immediately, existing network sessions, such as HMC connections, are stopped. If a firmware update is in progress, do not perform this operation. The new settings must be used to re-establish any network connections. Additional errors may also be logged if the system is powered on.

You can change the network configurations when the system is in any state. When the system is turned on, you can only view the network configurations.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To configure network interfaces, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand Network Services.
3. Select Network Configuration.
4. In the right pane, locate the interface that you want to change. Select the box corresponding to the Configure this interface? field of the identified interface. If this box is not selected, the corresponding field changes are ignored.
5. Select the Type of IP address from the following options:
   Static
   : The IP address, subnet mask, broadcast address, default gateway and first DNS server address must be entered. The second and third DNS server addresses are optional.

   Dynamic
   : No additional input is required.
6. Click Save settings to begin data validation.

   Attention: If incorrect network configuration information is entered, you may not be able to use the ASMI after the changes are made. To remedy this situation, you must reset the service processor to the default settings by removing the service processor assembly from the server and moving the reset jumpers. Resetting the service processor also resets all user IDs and passwords to their default values.

   The next screen allows you to verify the IP settings that have been entered. Click Continue to make the changes.

Parent topic: Configuring network services

Configuring network access

Specify which IP addresses will be allowed to access the server.

When you configure network access, you specify which IP addresses can access the service processor. You can specify a list of allowed IP addresses and a list of denied IP addresses.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To configure network access, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand Network Services.
3. Select Network Access. In the right pane, the IP address field displays the IP address of the server that your browser is running on and that connects to the ASMI.
4. Specify up to 16 addresses each for the list of allowed addresses and the list of denied addresses. `ALL` is a valid IP address.

   If a login is received from an IP address that matches a complete or partial IP address in the allowed list, access to the service processor is granted. Access to the service processor is not allowed if a login is received from an IP address that matches a complete or partial IP address from the denied list.

   Note: The allowed list takes priority over the denied list, and an empty denied list is ignored. `ALL` is not allowed in the denied list if the allowed list is empty.

5. Click Save settings to validate the data.

Parent topic: Configuring network services

Using extended services

Specify the IP address and directory path for remote systems.

ASMI allows you to mount a directory at a fixed mounting point on the service processor in order to enable utilities, such as telnet, ftp, and rsh. You can also clear the current mount settings. To mount a directory, the IP addresses of the remote system and path to the directory on the remote system must be provided. The targeted directory will be mounted at a fixed location on the host service processor. By default, the mount point is `/nfs`.

This option is beneficial for gathering additional debug information from a failing system. To enable utilities, such as telnet, the name and relative path to a shell script on the remote system along with the IP address and path to mount the directory on the remote system must be provided. This shell script, when executed on the host service processor, enables utilities such as telnet and ftp.

To access the extended services menu, your authority level must be an authorized service provider.

To configure extended services, do the following:

1. In the navigation area, expand Network Services.
2. Select Extended Services.
3. In the right pane, specify the IP address of the remote machine, directory path to mount on the remote machine, and relative path name of the shell script you desire to execute on the remote machine. The relative path of the shell script field is optional.
4. Click Save settings to mount the remote directory using your entered data or click Clear mount to unmount the previously mounted remote directory.

Parent topic: Configuring network services

Debugging virtual TTY

Debug virtual TTY from the master service processor.

You can gather additional debug information from a failing system by using the debug virtual server (DVS). The DVS enables communication with the server firmware and partition firmware. DVS allows a maximum of eight open connections. External interfaces such as the ASMI and service processor remote application can communicate with the server firmware and partition firmware through DVS. This communication is bidirectional. External interfaces can send a message to the server firmware and partition firmware through DVS.

DVS uses the partition ID and session ID to distinguish between the server firmware and partition firmware. The range for both the partition ID and session ID is 0 to 255. Clients, such as the ASMI, interact with DVS using a TCP/IP socket. Port 30002 on the service processor is used for this communication.

Two parameters, the partition ID and the session ID, must be specified to start communicating. After specifying both parameters, a telnet session must be opened to send messages. The telnet session must be started and messages must be sent within the time-out period of 15 minutes. If both actions are not taken within the time-out period, the connection is closed.

To perform this operation, your authority level must be authorized service provider.

To debug the virtual TTY, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand Network Services.
3. Select Debug Virtual TTY.
4. In the right pane, enter the partition and session IDs.
5. Click Save settings.

Parent topic: Configuring network services

Using on-demand utilities

Activate inactive processors or inactive system memory without restarting your server or interrupting your business.

Power On Demand (POD) allows you to permanently activate inactive processors or inactive system memory without requiring you to restart your server or interrupt your business. You can also view information about your POD resources.

Note: Use this topic if a hardware failure causes the system to lose its Power On Demand or Function On Demand purchased capabilities, and if there has never been an HMC managing the system. If an HMC is managing the system, use the HMC to perform the following tasks instead of the ASMI.

- **Order Power On Demand**
  Generate the system information that is required when ordering processor or memory activation features.
- **Activate Power On Demand**
  Activate processors or memory permanently with Power On Demand.
- **Resume server firmware after POD activation**
  Resume the booting process of the server firmware after the POD activation keys are entered.
- **Use Power On Demand commands**
  Run a command that is sent to the server firmware.
- **Viewing information about POD resources**
  View information about a system's available Power On Demand (POD) resources.

Parent topic: Managing your server using the Advanced System Management Interface

Order Power On Demand

Generate the system information that is required when ordering processor or memory activation features.

After you determine that you want to permanently activate some or all of your inactive processors or memory, you must order one or more processor or memory activation features. You then enter the resulting processor or memory-activation key that is provided by your hardware provider to activate your inactive processors or memory.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To order processor or memory activation features, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand On Demand Utilities.
3. Select POD (or CoD) Order Information. The server firmware displays the information that is necessary to order a Power On Demand activation feature.
4. Record the information that is displayed.
5. Click Continue.

Parent topic: Using on-demand utilities

Activate Power On Demand

Activate processors or memory permanently with Power On Demand.

When you obtain processor or memory activation features, you receive an activation key that you use to activate your inactive processors or memory.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To permanently activate some or all of your inactive processors or memory, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand On Demand Utilities.
3. Select POD (or CoD) Activation.
4. Enter the activation key into the field.
5. Click Continue to perform the specified operation.

Parent topic: Using on-demand utilities

Resume server firmware after POD activation

Resume the booting process of the server firmware after the POD activation keys are entered.

You can resume the server firmware after the POD activation keys are entered. Resuming the server firmware causes the POD key to become recognized and the hardware to become activated. This option allows the server to complete the startup process that has been delayed up to one hour in order to place the server into the *On Demand Recovery* state that was needed to enter the POD activation keys.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To resume the server firmware, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand On Demand Utilities.
3. Select POD (or CoD) Recovery.
4. Click Continue to perform the specified operation.

Parent topic: Using on-demand utilities

Use Power On Demand commands

Run a command that is sent to the server firmware.

As directed by your service provider, you can run a Power On Demand-related command that is sent to the server firmware.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To run a Power On Demand command, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand On Demand Utilities.
3. Select POD (or CoD) Command.
4. Enter the Power On Demand command into the field and click Continue. The response to the command from the server firmware is displayed.

Parent topic: Using on-demand utilities

Viewing information about POD resources

View information about a system's available Power On Demand (POD) resources.

When Power On Demand (POD) is activated on your system, you can view information about the POD processors, the memory that is allocated as POD memory, and Virtualization Engine technology resources.

To view the POD resource information, your authority level must be one of the following:

- Administrator
- Authorized service provider

To view information about POD resources, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand On Demand Utilities.
3. Select one of the following options for the type of information you want to view:
    a. POD Processor Information to view information about the POD processors
    b. POD Memory Information to view information about available POD memory
    c. POD Vet Information to view information about available Virtualization Engine technologies
    d. POD Capability Settings to view information about the POD capabilities that are enabled

Note: You can also view the POD capability settings from the Hardware Management Console (HMC).

Parent topic: Using on-demand utilities

Using concurrent maintenance utilities

Replace devices in your server without having to power off your server.

You can replace some devices in your server without having to power off your server.

- **Controlling power to IDE devices**
  Control power to your IDE devices.
- **Preparing the control panel**
  Prepare the control panel for concurrent maintenance.

Parent topic: Managing your server using the Advanced System Management Interface

Controlling power to IDE devices

Control power to your IDE devices.

You can control power to the integrated drive electronics (IDE) devices so that you can perform concurrent maintenance. Power to IDE devices, a pair at a time, can be turned on and off without affecting power to the rest of the devices in the server.

Attention: To avoid damaging the hardware, turn off the power to IDE devices before performing concurrent maintenance.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

Note: The IDE device control menu is available only when the system is powered on.

To control power to your IDE devices, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand Concurrent Maintenance.
3. Select IDE Device Control. The location code and current power state of each IDE device is displayed.
4. Click Power off to remove power from the IDE devices displayed in the list. To restore power to the IDE devices displayed in the list, click Power on.

Parent topic: Using concurrent maintenance utilities

Preparing the control panel

Prepare the control panel for concurrent maintenance.

You can prepare the control panel for concurrent maintenance by *logically* isolating the control panel. As a result, your firmware does not recognize the control panel as being active and you can remove it. Performing this operation prevents your hardware from becoming damaged while replacing the control panel. After a new control panel is installed, you can change the settings so that the hardware recognizes the new control panel.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

Note: The control panel menu is available only when the system is turned on.

For control-panel removal and replacement procedures, see Installing features and replacing parts.

To prepare the control panel for concurrent maintenance, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand Concurrent Maintenance.
3. Select Control Panel. You are asked to specify whether you want to remove or install the control panel.
4. Click Continue to display a list of all possible control-panel location codes.

   Note:

5. Click to select the appropriate location code of the control panel.
6. Click Save settings to perform the selected operation.

Attention: Do not reset the service processor, or remove then reapply power to the system, during this procedure. Doing so will result in the vital product data being lost and you will not be able to select from a list of control panel location codes when installing the new control panel. Resetting the service processor again might resolve the problem.

Parent topic: Using concurrent maintenance utilities

Troubleshooting the server using service aids

View and customize troubleshooting information with various service aids (such as viewing error logs and initiating service processor dumps).

This topic provides information about using the following ASMI service aids.

Note: The system ports are disabled when a Hardware Management Console (HMC) is attached to the server, and the server is booted beyond the service processor standby state.

- **Displaying error and event logs**
  Display a list of all of the error and event logs in the service processor.
- **Enabling serial port snoop**
  Specify parameters (including the snoop string) for enabling a serial port (system port) snoop.
- **Initiating a system dump**
  Control how frequently a system dump is performed and the amount of data collected from the hardware and server firmware.
- **Initiating a service processor dump**
  Enable or disable the service processor dump in addition to immediately initiating a service processor dump.
- **Initiating a partition dump**
  Enable or disable the service processor dump in addition to immediately initiating a partition dump.
- **Configuring a system port for call options**
  Configure the system port for use with the call-home and call-in options.
- **Configuring your modem**
  Configure your modem that is connected to the system port.
- **Configuring the call-home and call-in policy**
  Configure your system to call home and call in.
- **Testing the call-home policy**
  Perform a call-home test.
- **Rebooting the service processor**
  Reboot the service processor.
- **Restoring your server to factory settings**
  Restore firmware settings, network configuration, and passwords to their factory defaults.
- **Entering service processor commands**
  Enter commands to perform on the service processor.

Parent topic: Managing your server using the Advanced System Management Interface

Displaying error and event logs

Display a list of all of the error and event logs in the service processor.

You can view error and event logs that are generated by various service processor firmware components. The content of these logs can be useful in solving hardware or server firmware problems.

To perform this operation, your authority level must be one of the following:

- General
- Administrator
- Authorized service provider

Informational and error logs can be viewed by all authority levels. Hidden error logs can be viewed by authorized service providers.

The following table shows error log types that might be displayed, the conditions that make an error log specific to that error log type, and the user authority level that will allow you to view specific types of error logs:

Error log type	Conditions		User availability
	Severity	Action	
Informational logs	Informational	Report to operating system (OS) but not hidden	Available to all users
Error logs	Not informational	Report to OS but not hidden	Available to all users
Hidden logs	Not informational and informational	Report to OS, hidden, or both	Available only to the authorized service provider and users with higher authority.

To view error and event logs in summary or full detailed format, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Service Aids and click Error/Event Logs. If log entries exist, a list of error and event log entries is displayed in a summary view.
3. To view the full detail format of any of the logs listed, select the log's corresponding check box and click Show details. When multiple logs are selected, any action applies to each selected log. The full detail information might span several pages. The contents and layout of the full detail output is defined by the event or error logging component.
4. Click Mark as reported to mark platform error entries whose underlying causes have been resolved. By doing so, these entries are not reported to the operating system again when the system reboots. After they are marked, these errors can be overwritten by other errors logged in the service processor history log.

   Note: The Mark as reported button is available only when your authority level is an authorized service provider.

Parent topic: Troubleshooting the server using service aids

Enabling serial port snoop

Specify parameters (including the snoop string) for enabling a serial port (system port) snoop.

You can disable or enable a snoop operation on a system port. When enabled, data received on the selected port is examined, or *snooped*, as it arrives. You can also specify the snoop string, a particular sequence of bytes that resets the service processor if detected. The system port S1 serves as a "catchall" reset device.

Note: The system ports are disabled when a Hardware Management Console (HMC) is attached to the server, and the server is booted beyond the service processor standby state.

To perform this operation, your authority level must be one of the following:

- General
- Administrator
- Authorized service provider

To view and change the current Serial Port Snoop settings, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Service Aids and select Serial Port Snoop.
3. Disable or enable snooping on system port S1. The default is *Disabled*.
4. Enter the desired snoop string, up to 32 bytes, into the Snoop string field. The current value displayed is the default. Ensure that the string is not a commonly used string. A mixed-case string is recommended.
5. Click Update snoop parameters to update the service processor with the selected values.

   Note: After the snoop operation is correctly configured, at any point after the system is booted to AIX, the system uses the service processor reboot policy to restart whenever the reset string is typed on an ASCII terminal attached to system port S1.

Parent topic: Troubleshooting the server using service aids

Initiating a system dump

Control how frequently a system dump is performed and the amount of data collected from the hardware and server firmware.

You can initiate a system dump in order to capture overall system information, system processor state, hardware scan rings, caches, and other information. This information can be used to resolve a hardware or server firmware problem. A *system dump* can also be automatically initiated after a system malfunction, such as a checkstop or hang. It is typically 34 MB.

Note: Use this procedure only under the direction of your service provider.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To configure and initiate a system dump, do the following:

1. Perform a controlled shutdown of the operating system if possible.
2. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
3. In the navigation area, expand System Service Aids and click System dump.
4. From the selection list labeled Dump policy, select the policy to determine when an automatic system dump is collected.

   The dump policy is used whenever a system error condition is automatically detected by the system. In addition to the dump policy, the platform firmware determines whether a dump is recommended, based on the type of error that has occurred. This recommendation is combined with the dump policy to determine if a system dump will be initiated.

   The dump policy choices are the following:

   As needed
   : Collects the dump data only for specific reasons. This is the default setting for the dump policy.

   Always
   : Collects the dump data after the system locks up or after a checkstop. This setting overrides the firmware recommendation and forces a system dump, even when it is not recommended.

   Note: The dump policy only defines when a system dump is performed. It does not define what to dump nor the size of the information to be dumped. Those parameters are controlled by the Hardware content settings.

5. Select the policy to determine how much data to dump from the selection list labeled Hardware content.

   The system firmware makes a recommendation for the dump content based on the type of error that has occurred. This recommendation is combined with the hardware content to determine how much dump data is actually collected.

   The dump policy choices available are the following:

   - Automatic Collects dump data automatically. The firmware decides which dump content is best, depending on the type of failure. This is the default setting for the hardware content.
   - Minimum Collects the minimum amount of dump data. Collection of hardware dump data can be time-consuming. This selection allows the user to minimize the content of the hardware portion of the system dump. It also allows the system to reboot as quickly as possible.

     Note: If this option is selected, the debug data collected for some errors may be insufficient. The capturing of relevant error data for some errors may be sacrificed for less system downtime.

   - Medium Collects a moderate amount of hardware error data. More data is captured with this setting than the minimum setting, and less time is needed for dump data collection in comparison to the maximum setting.
   - Maximum Collects the maximum amount of hardware error data. This setting gives the most complete error coverage but requires more system downtime in relation to the other policies. It is expected to be used in rare cases by authorized service providers if you are willing to sacrifice reboot speed for error capture on a first failure, or if difficult problems are being analyzed.

     Note: If this option is selected, the collection of hardware dump data can be quite time-consuming, especially for systems with a large number of processors.

6. In the Server firmware content field, select the content level that indicates the amount of data to dump for the server firmware portion of the system dump.

7. Click Save settings to save the setting changes.

   To save the setting changes and instruct the system to immediately process a dump with the current settings, click Save settings and initiate dump.

   For information about copying, reporting, and deleting the dump, see Managing dumps in the Troubleshooting topic.

Parent topic: Troubleshooting the server using service aids

Initiating a service processor dump

Enable or disable the service processor dump in addition to immediately initiating a service processor dump.

Use this procedure only under the direction of your hardware service provider. With this function, you can preserve error data after a service processor application failure, external reset, or user request for a service processor dump. The existing service processor dump is considered valid if neither the server firmware nor Hardware Management Console (HMC) has collected the previous failure data.

To perform this operation, your authority level must be authorized service provider.

To enable or disable the service processor dump and view the status of the existing service processor dump, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Service Aids and click Service Processor Dump.
3. Select either Enable or Disable from the selection list. By default, the state is *Enable*. The current setting is displayed and the status of an existing service processor dump is displayed as valid or invalid.

   Note: You cannot perform a user-requested service processor dump when this setting is disabled.

4. Click Save settings to save the setting changes.

   To save the setting changes and instruct the system to immediately process a service processor dump with the current settings, click Save settings and initiate dump.

   For information about copying, reporting, and deleting the dump, see Managing dumps in the Troubleshooting topic.

Parent topic: Troubleshooting the server using service aids

Initiating a partition dump

Enable or disable the service processor dump in addition to immediately initiating a partition dump.

Use this procedure only under the direction of your hardware service provider. By initiating a partition dump, you can preserve error data that can be used to diagnose server firmware or operating system problems. The state of the operating system is saved on the hard disk and the partition restarts. This function can be used when the operating system is in an abnormal wait state, or endless loop, and the retry partition dump function is not available. The retry partition dump feature is present only on systems.

Attention: You may experience data loss when using this operation. This feature is only available on non-HMC managed systems that have the system server firmware in the *Running* state.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To perform a partition dump, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Service Aids and click Partition Dump.
3. Select Partition Dump. If your system is an server and the initial partition dump attempt failed, select Retry partition dump.

Parent topic: Troubleshooting the server using service aids

Configuring a system port for call options

Configure the system port for use with the call-home and call-in options.

You can configure the system ports used with the call-home and call-in features. You can also set the baud rate for all system ports.

Note: The system ports are disabled when a Hardware Management Console (HMC) is attached to the server, and the server is booted beyond the service processor standby state. Therefore, these menus are not present if the system is managed by an HMC, or if the system has no ports.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To configure the system ports, complete the following steps:

1. In the navigation area, expand System Service Aids and click Serial Port Setup. Two sections are displayed. The first section is labeled S1, which is the system port that is used with the call-home feature. The second section is labeled S2, which is the system port that is used with the call-in feature.
2. Modify the appropriate fields in the S1 and S2 sections.
   Baud rate
   : Select the baud rate for this system port. If a terminal is attached to this port, the settings must match. The speeds available are 50, 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 bps.
   Character size
   : Select the character size for this system port. If a terminal is attached to this port, the settings must match.
   Stop bits
   : Select the number of stop bits for thissystem port. If a terminal is attached to this port, the settings must match.

Parity
Select the parity for thissystem port. If a terminal is attached to this port, the settings must match.

3. Click Save settings to save the setting changes.

Parent topic: Troubleshooting the server using service aids

Configuring your modem

Configure your modem that is connected to the system port.

Note: The system ports are disabled when a Hardware Management Console (HMC) is attached to the server, and the server is booted beyond the service processor standby state.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To configure the modem, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Service Aids.
3. Select Modem Configuration. Two sections are displayed. The first section is labeled S1, which is the system port that is used with the call-home feature. The second section is labeled S2, which is the system port that is used with the call-in feature.
4. Modify the fields in the S1 and S2 sections.
   - Modem type Select the supported modem type from the selection list.
   - Modem reset command Enter the command to use to reset the modem to the power-on defaults.
   - Modem initialization command This command configures the modem for the required behavior. To ensure proper operation, result codes should be returned (ATQ0), echo should be disabled (ATE0), and result codes should be strings (ATV1). This setting is ignored if the modem type is not Custom.
   - Modem dial command This command is used for dialing a number. For example, ATDT for tone dialing. This setting is ignored if the modem type is not Custom.
   - Modem auto-answer command This command enables the modem to answer incoming calls. For example, ATS0=1. This setting is ignored if the modem type is not Custom.
   - Modem pager dial command Enter the modem pager dial command. This command is used to dial a pager. For example: ATDT%s,,,%s;ATH0.

     Note: Both `%s` strings are required. This setting is ignored if the modem type is not Custom.

   - Modem disconnect command Enter the modem disconnection command. This command is used to disconnect the call. For example, +++ATH0. This setting is ignored if the modem type is not Custom.
5. Click Save settings to save the modem configuration changes.

Parent topic: Troubleshooting the server using service aids

Configuring the call-home and call-in policy

Configure your system to call home and call in.

You can select which system port is used to call home and to call in, set various telephone numbers, and add customer information.

Note:

- The modem is required to be configured on call-in and call-home enabled system ports.
- The system ports are disabled when a Hardware Management Console (HMC) is attached to the server, and the server is booted beyond the service processor standby state.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To configure the call-in and call-home policies, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Service Aids.
3. Select Call-in/Call-home.
4. Enter the desired text into the specified fields.
    - Call-home policy
        - Call-home serial port Select a system port for call-home or select Disabled to disable call-home.
        - Call-in serial port Select a system port for call-in or select Disabled to disable call-in.
        - Call-home dialing policy Select the dialing policy for call-home. Select First to call the telephone numbers in sequence and to stop at the first successful call-home, or select All to call all of the telephone numbers.
        - Number of retries This setting is the number of times the server should retry calls that were unsuccessful.
    - Telephone numbers
        - Service center telephone number This is the number of the service center computer. The service center usually includes a computer that takes calls from servers with call-out capability. This computer is referred to as the catcher. The catcher expects messages in a specific format to which the service processor conforms. For more information about the format and catcher computers, refer to the readme file in the AIX /usr/samples/syscatch directory. Contact your authorized service provider for the correct service center telephone number to enter. Until you have that number, leave this field unassigned.
        - Customer administration center telephone number This is the number of the system administration center computer (catcher) that receives problem calls from servers. Contact your system administrator for the correct telephone number to enter here. Until you have that number, leave this field unassigned.
        - Digital pager telephone number This is the number for a numeric pager carried by someone who responds to problem calls from your server. Contact your administration center representative for the correct telephone number to enter.
        - Pager numeric data Enter the numeric data to be sent during a pager call.
    - Customer account
        - **Customer RETAIN account number** This is the number assigned by your RETAIN service provider for record keeping and billing. Enter your account number.
        - **Customer RETAIN login user ID** Enter the RETAIN login user ID. Leave this field unassigned if your service provider does not use RETAIN.
        - **Customer RETAIN login password** Enter the RETAIN account password. Leave this field unassigned if your service provider does not use RETAIN.

- ◊ **Primary RETAIN server IP address** Enter the IP address of the primary RETAIN server.
- ◊ **Secondary RETAIN server IP address** Enter the IP address of the secondary RETAIN server.
- ◊ **Customer site user ID** Enter the user ID for your problem reporting center.
- ◊ **Customer site password** Enter the password for your problem reporting center.

♦ Customer company information
- ◊ Company name
- ◊ Street address
- ◊ City and state
- ◊ Zip/postal code
- ◊ Country

5. Click Save settings to save changes.

Parent topic: Troubleshooting the server using service aids

Testing the call-home policy

Perform a call-home test.

You can test the call-home policy configuration after the modem is installed and configured correctly.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To test your call-home policy configuration, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Service Aids.
3. Select Call-Home Test.
4. Click Initiate call-home test. A test of the call-home system is performed as specified by the current port and modem selections.

Parent topic: Troubleshooting the server using service aids

Rebooting the service processor

Reboot the service processor.

In critical system situations, such as during system hangs, you can reboot the service processor. It is recommended that you perform this task only when directed by your service provider.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To reboot your service processor, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Service Aids.

3. Select Reset Service Processor.
4. Click Continue to perform the reboot.

Parent topic: Troubleshooting the server using service aids

Restoring your server to factory settings

Restore firmware settings, network configuration, and passwords to their factory defaults.

You can reset all the factory settings on your server to the factory default settings, or you can choose to reset specific settings by using the following options:

- Reset all settings OR
- Reset the service processor settings
- Reset the server firmware settings
- Reset the PCI bus configuration

If you choose to reset all settings, all three of these actions are performed resulting in the service processor settings, the server firmware settings, and the PCI bus configuration being reset in one operation.

Note: If redundant service processors are installed and enabled, whichever type of reset operation that you perform on the primary service processor will also be performed on the secondary service processor.

Attention: It is generally recommended that you reset your server settings to the factory default only when directed by your service provider. Before you reset all settings, make sure you have manually recorded all settings that need to be preserved. This operation can be performed only if the identical level of firmware exists on both the permanent firmware boot side, also known as the P side, and the temporary firmware boot side, also known as the T side.

Resetting the service processor settings results in the loss of all system settings (such as the HMC access and ASMI passwords, time of day, network configuration, and hardware deconfiguration policies) that you may have set through user interfaces.

Resetting the server firmware settings results in the loss of all of the partition data that is stored on the service processor.

Resetting the PCI bus configuration results in the following sequence of events:

- The service processor instructs the server firmware to power on and enter into a standby state.
- When the server firmware has entered into the standby state, the PCI bus configuration settings are cleared.
- The server firmware then powers off and the service processor is in the standby state.

Resetting all settings results in the loss of system settings as described for each option in the preceding paragraphs. Also, you will lose the system error logs and partition-related information.

To restore factory default settings, your authority level must be one of the following:

- Administrator
- Authorized service provider

To restore factory default settings, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Service Aids.
3. Select Factory Configuration.
4. Select the options that you want to restore to factory settings.
5. Click Continue. The service processor reboots after all settings have been reset.

Parent topic: Troubleshooting the server using service aids

Entering service processor commands

Enter commands to perform on the service processor.

You can enter commands to perform on the service processor. Currently, no syntactical validation is performed on the command string that is entered. As a result, ensure that the command is entered correctly before initiating the action.

To perform this operation, your authority level must be an authorized service provider.

To enter service processor commands, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click Log In.
2. In the navigation area, expand System Service Aids.
3. Select Service Processor Command Line.
4. Enter a valid command that does not exceed 80 characters.

   Note: Entering an invalid command may hang the system. If this condition occurs, it is recommended that you reset the service processor.

5. Click Execute to perform the command on the service processor.

Parent topic: Troubleshooting the server using service aids

Technical publication remarks form

Title :	ESCALA POWER5 Hardware Information Managing your server using the Advanced System Management Interface

Reference N° :	86 A1 36EW 00	**Date:**	July 2006

ERRORS IN PUBLICATION

SUGGESTIONS FOR IMPROVEMENT TO PUBLICATION

Your comments will be promptly investigated by qualified technical personnel and action will be taken as required.
If you require a written reply, please include your complete mailing address below.

NAME : _____ Date : _____

COMPANY : _____

ADDRESS : _____

_____

Please give this technical publication remarks form to your BULL representative or mail to:

Bull - Documentation Dept.
1 Rue de Provence
BP 208
38432 ECHIROLLES CEDEX
FRANCE
info@frec.bull.fr

Technical publications ordering form

To order additional publications, please fill in a copy of this form and send it via mail to:

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

Phone: +33 (0) 2 41 73 72 66
FAX: +33 (0) 2 41 73 70 66
E-Mail: srv.Duplicopy@bull.net

CEDOC Reference #	Designation	Qty
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		

[_ _] : The latest revision will be provided if no revision number is given.

NAME: ______________________________ Date: __________

COMPANY: ______________________________

ADDRESS: ______________________________

____

PHONE: ______________________ FAX: ______________

E-MAIL: ______________________________

For Bull Subsidiaries:

Identification: ______________________________

For Bull Affiliated Customers:

Customer Code: ______________________________

For Bull Internal Customers:

Budgetary Section: ______________________________

For Others: Please ask your Bull representative.

BLANK

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

REFERENCE
86 A1 36EW 00