

Remote Supervisor Adapter II



# User's Guide



Remote Supervisor Adapter II



# User's Guide

**Note:** Before using this information and the product it supports, read the general information in Appendix B, "Notices", on page 53.

**Second Edition (June 2003)**

**© Copyright International Business Machines Corporation 2003. All rights reserved.**

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

---

# Contents

<b>Chapter 1. Introduction</b> . . . . .	1
Remote Supervisor Adapter II features . . . . .	1
Web browser requirements . . . . .	2
Notices used in this book . . . . .	2
<b>Chapter 2. Opening and using the Web browser interface</b> . . . . .	3
Logging in to the Remote Supervisor Adapter II . . . . .	3
Remote Supervisor Adapter II action descriptions. . . . .	5
<b>Chapter 3. Configuring your Remote Supervisor Adapter II.</b> . . . . .	9
Setting system information . . . . .	10
Setting server timeouts . . . . .	11
Setting the date and time . . . . .	14
Creating a login profile . . . . .	14
Setting the global login settings . . . . .	16
Configuring remote alert settings . . . . .	16
Configuring remote alert recipients. . . . .	17
Forwarding alerts . . . . .	19
Setting remote alert attempts. . . . .	20
Setting remote alerts. . . . .	21
Setting local events . . . . .	23
Configuring the serial port . . . . .	24
Configuring an Ethernet connection to the Remote Supervisor Adapter II . . . . .	26
Configuring network protocols . . . . .	29
Configuring SNMP . . . . .	29
Configuring SMTP. . . . .	31
Using the configuration file . . . . .	32
Backing up your current configuration . . . . .	32
Restoring and modifying your ASM configuration . . . . .	33
Restoring ASM defaults. . . . .	33
Restarting ASM. . . . .	34
Logging off . . . . .	34
<b>Chapter 4. Monitoring remote server status</b> . . . . .	35
Viewing system health . . . . .	35
Viewing the event log . . . . .	39
Viewing vital product data . . . . .	40
<b>Chapter 5. Performing Remote Supervisor Adapter II tasks</b> . . . . .	43
Server power and restart activity . . . . .	43
Remotely controlling the power status of a server . . . . .	44
Remote control . . . . .	45
Remote console . . . . .	45
Remote disk . . . . .	46
Updating firmware. . . . .	48
Accessing remote adapters through an ASM interconnect network . . . . .	49
<b>Appendix A. Getting help and technical assistance</b> . . . . .	51
Before you call . . . . .	51
Using the documentation . . . . .	51
Getting help and information from the World Wide Web . . . . .	51
Software service and support . . . . .	52
Hardware service and support . . . . .	52

<b>Appendix B. Notices</b> . . . . .	53
Edition notice . . . . .	53
Trademarks . . . . .	54
<b>Index</b> . . . . .	55

---

## Chapter 1. Introduction

This manual explains how to use the functions of the IBM® Remote Supervisor Adapter II when you install it in an IBM @server™ xSeries™ server. The IBM Remote Supervisor Adapter II is one of the products in the Advanced System Management (ASM) family. The Remote Supervisor Adapter II provides the following functions:

- Around-the-clock remote access and system management of your server
- Remote management independent of the status of the managed server
- Remote control of hardware and operating systems
- Web-based management with standard Web browsers

---

### Remote Supervisor Adapter II features

The Remote Supervisor Adapter II has the following standard features:

- Continuous health monitoring and control
- Automatic notification and alerts
- Nonvolatile event log showing time stamped entries
- Remote access through Ethernet and ASM interconnect peer-to-peer network
- Secure socket layer (SSL) security for remote management access
- Simple Network Management Protocol (SNMP) trap support
- E-mail alerts
- Alphanumeric or numeric pager alerts
- Domain Name System (DNS) server support
- Dynamic Host Configuration Protocol (DHCP) support
- Remote power control
- Operating-system-failure screen capture
- Remote firmware update
- Access to critical server settings
- Access to server vital product data (VPD)
- Redirection of the server console
- Virtually attaching a remote diskette drive, CD-ROM drive, or disk image to a server

---

## Web browser requirements

The Remote Supervisor Adapter II supports the following Web browsers for remote access. The Web browser that you use must be Java™-enabled and must support JavaScript™.

- Microsoft® Internet Explorer version 4.0 (with Service Pack 1), or later
- Netscape Navigator version 4.72, or later (version 6.x is not supported)

**Notes:**

1. Java plug-in version 1.4 or later is required.
2. The Remote Supervisor Adapter II Web interface does not support the double-byte character set (DBCS) languages.

---

## Notices used in this book

The following notices are used in the documentation:

- **Notes:** These notices provide important tips, guidance, or advice.
- **Important:** These notices provide information or advice that might help you avoid inconvenient or problem situations.
- **Attention:** These notices indicate potential damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage could occur.



---

## Chapter 2. Opening and using the Web browser interface

To access the Remote Supervisor Adapter II remotely using the Remote Supervisor Adapter II Web interface, you must log in to the adapter. This chapter describes the login procedures and describes the actions you can perform from the Remote Supervisor Adapter II Web interface.

---

### Logging in to the Remote Supervisor Adapter II


Complete the following steps to access the Remote Supervisor Adapter II through the Remote Supervisor Adapter II Web interface:

1. Open a Web browser. In the address or URL field, type the IP address or host name of the Remote Supervisor Adapter II to which you want to connect.

**Note:** You can obtain the IP address or host name from the server BIOS or from your network administrator.

The Enter Network Password window opens.

**Note:** The values in the following window are examples. Your settings will be different.



Enter Network Password

Please type your user name and password.

Site: 9.67.41.147

Realm: Local System

User Name

Password

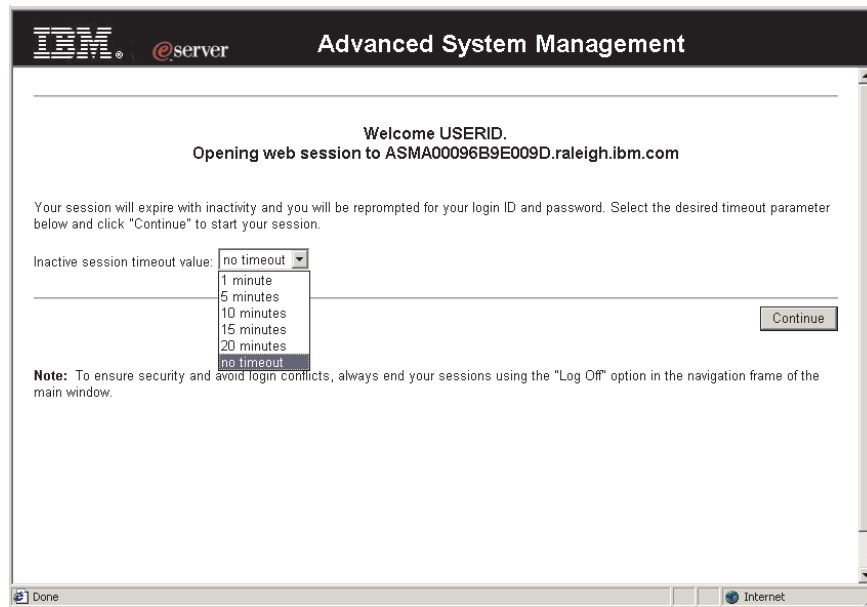
Save this password in your password list

OK Cancel

2. Type your user name and password in the Enter Network Password window. If you are using the Remote Supervisor Adapter II for the first time, you can obtain your user name and password from your system administrator. All login attempts are documented in the event log. A welcome page opens in your browser.

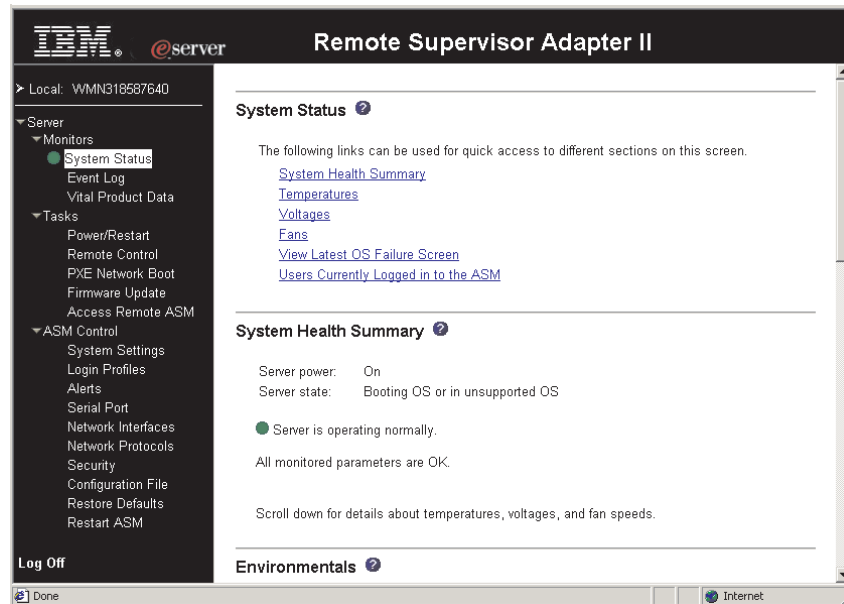
**Note:** The Remote Supervisor Adapter II is set initially with a user name of USERID and password of PASSWORD (with a zero, not an O). This user has read/write access. Change this default password during your initial

configuration for enhanced security.



3. Select a timeout value from the drop-down list in the field provided. If your browser is inactive for that number of minutes, the Remote Supervisor Adapter II logs you off the Remote Supervisor Adapter II Web interface.
4. Click **Continue** to start the session.

The browser opens the System Health page, which gives you a quick view of the server status.



For descriptions of the actions that you can perform from the links in the left navigation pane of the Remote Supervisor Adapter II Web interface, see “Remote Supervisor Adapter II action descriptions” on page 5. Then, go to Chapter 3, “Configuring your Remote Supervisor Adapter II”, on page 9.

## Remote Supervisor Adapter II action descriptions

Table 1 lists the actions available when you are logged in to the Remote Supervisor Adapter II.

Table 1. Remote Supervisor Adapter II actions

Link	Action	Description
System Status	View system health for a server, view the operating-system-failure screen capture, and view the users logged in to the Remote Supervisor Adapter II	You can monitor the server power and state and the temperature, voltage, and fan status of your server on the System Health page. You can also view the image of the last operating-system-failure screen capture and the users logged in to the Remote Supervisor Adapter II.
Event Log	View event logs for remote servers	The Event Log page contains entries that are currently stored in the server event log and power-on self-test (POST) event log. Information about all remote access attempts and dial-out events are recorded in the event log. All events in the log are time stamped using the Remote Supervisor Adapter II date and time settings. Some events will also generate an alert, if configured to do so on the Alerts page. You can sort and filter events in the event log.
Vital Product Data	View the server VPD	Upon server startup, the Remote Supervisor Adapter II collects system information and basic input/output system (BIOS) information, and server component vital product data (VPD) and stores it in nonvolatile memory. This data is available from the Vital Product Data page.
Power/Restart	Remotely turn on or restart a server	The Remote Supervisor Adapter II provides full remote power control over your server with power-on, power-off, and restart actions. In addition, power-on and restart statistics are captured and displayed to show server hardware availability.
Remote Control	Redirect the server video console and use your computer disk drive or disk image as a drive on the server	From the Remote Control page, you can start the Remote Control function. Using the Remote Control function, you can redirect the server console to your computer, and you can mount one of your computer disk drives, such as the CD-ROM drive or the diskette drive, on the server. When you have redirected the server console, you can use your mouse and keyboard to control the server. When you have mounted a disk, you can use it to restart the server and to update firmware on the server. You can use the Remote Console function to access the mounted disk, which will appear as a Universal Serial Bus (USB) disk drive attached to the server.
PXE Network Boot	Change the host server startup (boot) sequence for the next restart to attempt a PXE/DHCP network startup.	If your server BIOS and Preboot Execution Environment (PXE) boot agent utility are properly defined, from the PXE Network Boot page you can change the host server startup (boot) sequence for the next restart to attempt a PXE/DHCP network startup. The host startup sequence will be altered only if the host is not under Privileged Access Protection (PAP). After the next restart occurs, the check box on the PXE Network Boot page will be cleared.
Firmware Update	Update firmware on the Remote Supervisor Adapter II	Use the options on the Firmware Update page to update firmware of the Remote Supervisor Adapter II.

Table 1. Remote Supervisor Adapter II actions (continued)

Link	Action	Description
Access Remote ASM	Access other service processors on the ASM interconnect network	From the Access Remote ASM page, you can view a list of service processors present on the ASM interconnect network and establish a connection to any of those systems. <b>Note:</b> <i>Service processors</i> are Remote Supervisor Adapter IIs, Remote Supervisor Adapters, ASM processors, ASM PCI adapters, and integrated system management processors (ISMPs).
System Settings	View and change the Remote Supervisor Adapter II system settings	You can configure the server location and general information, such as the name of the Remote Supervisor Adapter II, the operating system that the Remote Supervisor Adapter II will support (Windows or Linux), server timeout settings, and contact information for the Remote Supervisor Adapter II, from the System Settings page.
	Set the Remote Supervisor Adapter II clock	You can set the Remote Supervisor Adapter II clock that is used for time stamping the entries in the event log.
Login Profiles	Configure the Remote Supervisor Adapter II login profiles	You can define 12 login profiles that enable access to the Remote Supervisor Adapter II, and define global login settings that apply to all login profiles.
Alerts	Configure remote alerts and remote alert recipients	You can configure the Remote Supervisor Adapter II to generate and forward alerts for a number of different events. You can configure the alerts that are monitored and the recipients that are notified on the Alerts page.
	Configure local events	You can set the local events monitored by the Remote Supervisor Adapter II, for which notifications are sent to the IBM Director console.
	Configure alert settings	You can establish global settings that apply to all remote alert recipients, such as the number of alert retries and the delay between the retries.
Serial Port	Configure the Remote Supervisor Adapter II serial port and modem settings	From the Serial Port page, you can configure the serial port and modem settings used by the Remote Supervisor Adapter II.
Network Interfaces	Configure the network interfaces of the Remote Supervisor Adapter II	From the Network Interfaces page, you can configure network-access settings for the Ethernet connection on the Remote Supervisor Adapter II. The Remote Supervisor Adapter II Ethernet connection enables remote access using a Web browser.
Network Protocols	Configure the network protocols of the Remote Supervisor Adapter II	You can configure Simple Network Management Protocol (SNMP), Domain Name System (DNS), and Simple Mail Transfer Protocol (SMTP) settings used by the Remote Supervisor Adapter II from the Network Protocols page.
Security	Configure the secure socket layer (SSL) for the Web interface	You can enable or disable SSL for the Web interface and manage the SSL certificate that is used.
Configuration File	Back up and restore the Remote Supervisor Adapter II configuration	You can back up, modify, and restore the configuration of the Remote Supervisor Adapter II, and view a configuration summary, from the Configuration File page.

Table 1. Remote Supervisor Adapter II actions (continued)

Link	Action	Description
Restore Defaults	Restore the Remote Supervisor Adapter II defaults	<b>Attention:</b> When you click <b>Restore Defaults</b> , all of the modifications you made to the Remote Supervisor Adapter II are lost.  You can reset the configuration of the Remote Supervisor Adapter II to the factory defaults.
Restart ASM	Restart the Remote Supervisor Adapter II	You can restart the Remote Supervisor Adapter II.
Log off	Log off the Remote Supervisor Adapter II	You can log off your connection to the Remote Supervisor Adapter II.

You can click the **View Configuration Summary** link, which is available on most pages, to quickly view the configuration of the Remote Supervisor Adapter II.



---

## Chapter 3. Configuring your Remote Supervisor Adapter II

Use the links under ASM Control in the navigation pane to configure the Remote Supervisor Adapter II.

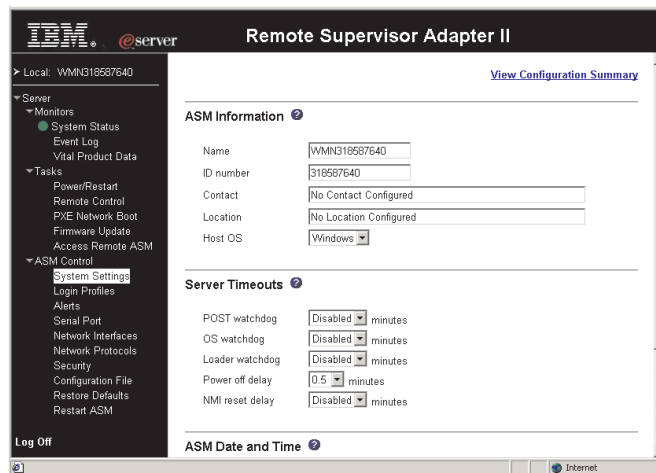
- From the System Settings page, you can:
    - Set system information
    - Select the operating system to support (Windows or Linux)
  - **Attention:**
    - For the Remote Supervisor Adapter II to function properly, the specified operating system must match the operating system of the server in which the Remote Supervisor Adapter II is installed.
    - Set this selection to Linux before attempting to install Linux device drivers.
  - Set server timeouts
  - Set ASM date and time
  - From the Login Profiles page, you can:
    - Set login profiles to control access to the Remote Supervisor Adapter II
    - Configure global login settings, such as the lockout period after unsuccessful login attempts
  - From the Alerts page, you can:
    - Set integrated system management processor (ISMP) alert forwarding
    - Configure remote alert recipients
    - Set the number of remote alert attempts
    - Select the delay between alerts
    - Select which alerts will be sent and how they will be forwarded
  - From the Serial Port page, you can:
    - Configure the serial port of the Remote Supervisor Adapter II
    - Configure advanced modem settings
  - From the Network Interfaces page, you can:
    - Set up the Ethernet connection for the Remote Supervisor Adapter II
  - From the Network Protocols page, you can:
    - Configure SNMP setup
    - Configure DNS setup
    - Configure SMTP setup
  - From the Security page, you can view or change the secure socket layer (SSL) settings. You can enable or disable (the default) SSL, and choose between self-signed certificates and certificates provided by a certificate authority (CA).
- Note:** The first time you select **Security**, you are directed to an IBM Web page for downloading the SSL installation key. After you load the key, the Security choice functions as described.
- From the Configuration File page, you can back up, modify, and restore the configuration of the Remote Supervisor Adapter II.
  - From the Restore Defaults page, you can reset the Remote Supervisor Adapter II configuration to the factory defaults.
  - From the Restart ASM page, you can restart the Remote Supervisor Adapter II.

## Setting system information

Complete the following steps to set your Remote Supervisor Adapter II system information:

1. Log in to the Remote Supervisor Adapter II where you want to set the system information. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.
2. In the navigation pane, click **System Settings**. A page similar to the one in the following illustration is displayed.

**Note:** The available fields in the System Settings page are determined by the accessed remote server.



3. In the **Name** field in the ASM Information section, type the name of the Remote Supervisor Adapter II.

Use the **Name** field to specify a name for the Remote Supervisor Adapter II in this server. The name is included with e-mail, SNMP, and alphanumeric pager alert notifications to identify the source of the alert.

### Notes:

- a. If you plan to set up an SMTP server for e-mail alert notifications, be sure that the name in the **Name** field is valid as part of an e-mail address (for example, there are no spaces).
  - b. Your Remote Supervisor Adapter II name (in the **Name** field) and the IP host name of the Remote Supervisor Adapter II (in the **Host Name** field on the Network Interfaces page) do not automatically share the same name because the **ASM Name** field is limited to 15 characters. The **Host Name** field can contain up to 63 characters. To minimize confusion, set the **ASM Name** field to the nonqualified portion of the IP host name. The nonqualified IP host name consists of up to the first period of a fully qualified IP host name. For example, for the fully qualified IP host name `asmcard1.us.company.com`, the nonqualified IP host name is `asmcard1`. For information about your host name, see “Configuring an Ethernet connection to the Remote Supervisor Adapter II” on page 26.
4. In the **ID number** field, assign the Remote Supervisor Adapter II a unique identification number.
  5. In the **Contact** field, type the contact information. For example, you can specify the name and phone number of the person to contact if there is a problem with this server. You can type a maximum of 47 characters in this field.



**Note:** The **Contact** field is not available for all servers.

- In the **Location** field, type the location of the server. Include in this field sufficient detail to quickly locate the server for maintenance or other purposes. You can type a maximum of 47 characters in this field.

**Note:** The **Location** field is not available for all servers.

- In the **HOST O/S** menu, click the type of operating system that is running on the server.

**Attention:**

- The operating system that you specify must match the operating system in the server for the Remote Supervisor Adapter II to function properly.
  - Set this selection to **Linux** before attempting to install Linux device drivers. The default setting is **Windows**.
- Scroll to the bottom of the page and click **Save**.

## Setting server timeouts

Complete the following steps to set your server timeout values:

- Log in to the Remote Supervisor Adapter II where you want to set the server timeouts. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.
- In the navigation pane, click **System Settings** and scroll down to the Server Timeouts section.

A page similar to the one in the following illustration is displayed.

---

**Server Timeouts** ⓘ

POST watchdog	Disabled	minutes
O/S watchdog	Disabled	minutes
Loader watchdog	Disabled	minutes
Power off delay	0.5	minutes
NMI reset delay	Disabled	minutes

---

You can set the Remote Supervisor Adapter II to respond automatically to the following events:

- Halted power-on self-test
  - Halted operating system
  - Failure to load operating system
  - Power-off delay to shut down operating system
  - Nonmaskable interrupt
- Enable the server timeouts that correspond to the events you want the Remote Supervisor Adapter II to respond to automatically.

### POST watchdog

Use the **POST watchdog** field to specify the number of minutes that the Remote Supervisor Adapter II will wait for the server to complete a power-on self-test (POST). If the server being monitored fails to complete a POST within the specified time, the Remote Supervisor Adapter II generates a POST timeout alert and automatically restarts the server. The POST watchdog is then automatically disabled until the

operating system is shut down and the server is power cycled (or until the operating system starts and the device driver successfully loads).

**Note:** Power cycling differs from shutting down and restarting the operating system in that power cycling removes power from the server completely; for example, you can power cycle the server by disconnecting it from the power source.

To set the POST timeout value, select a number from the menu. To turn off this option, select **Disabled**.

**Note:** If the **POST Time-out** check box is selected in the Remote Alerts section of the Remote Alerts page, the Remote Supervisor Adapter II attempts to forward the alert to all configured remote alert recipients. Also, the POST watchdog requires a specially constructed POST routine available only on specific IBM servers. If this routine does not exist on your server, all settings in this field are ignored.

For more information about POST routines, see the documentation that comes with your server.

### **O/S watchdog**

Use the **O/S watchdog** field to specify the number of minutes between checks of the operating system by the Remote Supervisor Adapter II. If the operating system fails to respond to one of these checks, the Remote Supervisor Adapter II generates an O/S timeout alert and restarts the server. After the server is restarted, the O/S watchdog is disabled until the operating system is shut down and the server is power cycled.

To set the O/S watchdog value, select a time interval from the menu. To turn off this watchdog, select **Disabled**. To capture operating-system-failure screens, you must enable the watchdog in the **O/S watchdog** field and select the **O/S Time-out** check box in the Remote Alerts section of the Alerts page.

#### **Notes:**

- a. The O/S watchdog feature requires that the Remote Supervisor Adapter II device driver is installed on the server. For information about installing device drivers, see the *Remote Supervisor Adapter II Installation Guide*.
- b. If the **O/S Time-out** check box is selected in the Remote Alerts section of the Alerts page, the Remote Supervisor Adapter II will attempt to send an alert to all configured remote alert recipients.

### **Loader watchdog**

Use the **Loader watchdog** field to specify the number of minutes that the Remote Supervisor Adapter II waits between the completion of POST and the starting of the operating system. If this interval is exceeded, the Remote Supervisor Adapter II generates a loader timeout alert and automatically restarts the server. After the server is restarted, the loader timeout is automatically disabled until the operating system is shut down and the server is power cycled (or until the operating system starts and the device driver successfully loads).

To set the loader timeout value, select the time limit that the Remote Supervisor Adapter II will wait for operating-system starting to be completed. To turn off this watchdog, select **Disabled**.

**Notes:**

- a. Before you start (boot) an operating system that does not have the Remote Supervisor Adapter II device drivers installed (this can also include using a flash update diskette), be sure to select **Disabled** in the **Loader watchdog** field to prevent an unwanted restart of your server.
- b. If the **Loader Time-out** check box is selected in the Remote Alerts section of the Alerts page, the Remote Supervisor Adapter II will send an alert to all configured remote alert recipients.

**Power off delay**

**Attention:** Read the following information to prevent the loss of data or damage to data when you perform a remote shutdown of your operating system:

If the Windows® 2000, Red Hat Linux, or SuSE Linux operating system is installed on your server, you need to install only the Remote Supervisor Adapter II device driver to support remote operating-system shutdown.

**Note:** If the value is less than 45 seconds in the **Power off delay** field, the device driver will adjust the value to 45 seconds when the device driver loads. You can decrease the power-off delay value after the server has started, but the device driver will reset it to 45 seconds on the next server restart. The device driver will not change a power-off delay value that is 45 seconds or greater.

Use the **Power off delay** field to specify the number of minutes that the Remote Supervisor Adapter II will wait for the operating system to shut down before turning off the server.

Shut down your server to determine how long it takes to shut down. Add a time buffer to that value and use it as your power-off delay setting to ensure that the operating system has time for an orderly shutdown before power is removed from the server.

To set the power-off delay value, select the time from the menu.

**NMI reset delay**

Use the **NMI reset delay** field to specify the length of time, in minutes, that the Remote Supervisor Adapter II waits to automatically restart the server after a nonmaskable interrupt (NMI) is triggered. A nonmaskable interrupt usually indicates a critical error such as a hardware fault. A nonmaskable interrupt usually signals a parity error in the memory subsystem.

To disable the automatic server restart after a nonmaskable interrupt, select **Disabled**.

**Note:** The **NMI reset delay** field is not available on all servers.

4. Scroll to the bottom of the page and click **Save**.

## Setting the date and time

The Remote Supervisor Adapter II contains its own real-time clock to time stamp all events that are logged in the event log. Alerts sent by e-mail, LAN, and SNMP use the real-time clock setting to time stamp the alerts. The clock settings support Greenwich mean time (GMT) offsets and daylight saving time (DST) for added ease-of-use for administrators managing systems remotely over different time zones. You can remotely access the event log even if the server is turned off or disabled. This facilitates immediate problem determination and resolution.

Complete the following steps to verify the date and time settings of the Remote Supervisor Adapter II:

1. Log in to the Remote Supervisor Adapter II where you want to set the ASM date and time values. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.
2. In the navigation pane, click **System Settings** and scroll down to the **ASM Date and Time** section, which shows the date and time when the Web page was generated.
3. To override the date and time settings and to enable daylight saving time (DST) and Greenwich mean time (GMT), click **Set ASM Date and Time**. A page similar to the one in the following illustration displays.

---

### ASM Date and Time

Date (mm/dd/yyyy)  /  /

Time (hh:mm:ss)  :  :

GMT offset

Automatically adjust for daylight saving changes

---

4. In the **Date** field, type the numbers of the current month, day, and year in the matching entry fields.
5. In the **Time** field, type the numbers corresponding to the current hour, minutes, and seconds in the appropriate entry fields. The hour (hh) must be a number from 00 to 23 as represented on a 24-hour clock. The minutes (mm) and seconds (ss) must be numbers from 00 to 59.
6. In the **GMT offset** field, type the number that specifies the offset in hours from Greenwich mean time (GMT), corresponding to the time zone where the server is located.
7. Select or clear the **Automatically adjust for daylight saving changes** check box to specify whether the Remote Supervisor Adapter II clock will automatically adjust when the local time changes between standard time and daylight saving time.
8. Scroll to the bottom of the page and click **Save**.

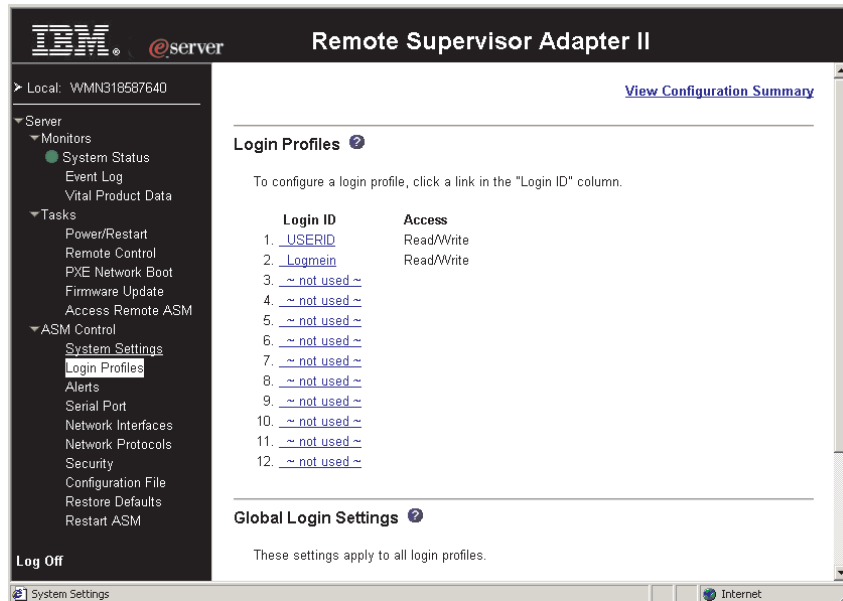
---

## Creating a login profile

Use the Login Profiles table to view, configure, or change individual login profiles. Use the links in the Login ID column to configure individual login profiles. You can define up to 12 unique profiles. Each link in the Login ID column is labeled with the configured login ID for that particular profile. If you have not configured a profile, the name of the link by default will be ~ not used ~.

Complete the following steps to configure a login profile:

1. Log in to the Remote Supervisor Adapter II where you want to create a login profile. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.
2. In the navigation pane, click **Login Profiles**. The Login Profiles page displays each login ID and the login access level, as shown in the following illustration.



**Note:** By default, the Remote Supervisor Adapter II is configured with one login profile that enables remote access using a login user ID of USERID and a password of PASSWORD (the 0 is a zero not an O). To avoid a potential security exposure, change this default login profile during the initial setup of the Remote Supervisor Adapter II.

3. Click one of the unused login profile links. An individual profile window similar to the one in the following illustration opens.

**Login Profile 2** ?

Login ID

Authority level

Password

Confirm password

4. In the **Login ID** field, type the name of the profile.  
You can type a maximum of 15 characters in the **Login ID** field. Valid characters are uppercase and lowercase letters, numbers, periods, and underscores.

**Note:** This login ID is used to grant remote access to the Remote Supervisor Adapter II.

5. In the **Authority level** field, select either **Read Only** or **Read/Write** to set the access rights for this login ID.

### **Read Only**

You can use the **Read Only** option to view a window but not to make changes. Additionally, if you log in with a read-only ID, you cannot perform file transfers, power and restart actions, or remote control functions.

### **Read/Write**

You can use the **Read/Write** option to take all available actions provided by the interface, including setting up a user ID and turning off the server.

6. In the **Password** field, assign a password to the login ID.

A password must contain at least five characters, one of which must be a nonalphabetic character. Null or empty passwords are accepted.

**Note:** This password is used with the login ID to grant remote access to the Remote Supervisor Adapter II.

7. In the **Confirm Password** field, type the password again.
8. Click **Save** to save your login ID settings.

---

## **Setting the global login settings**

Complete the following steps to set conditions that apply to all login profiles for the Remote Supervisor Adapter II:

1. Log in to the Remote Supervisor Adapter II for which you want to set the global login settings. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.
2. In the navigation pane, click **Login Profiles**.
3. Scroll down to the Global Login Settings section.
4. To allow remote users to dial in to the Remote Supervisor Adapter II through a serial connection, select **Enabled** in the **Logins through a modem connection** field.
5. In the **Lockout period after five login failures** field, specify how long, in minutes, the Remote Supervisor Adapter II will prohibit remote login attempts, if more than five sequential failures to log in remotely are detected.

---

## **Configuring remote alert settings**

You can configure remote alert recipients, the number of alert attempts, incidents that trigger remote alerts, and local alerts from the **Alerts** link on the navigation pane.

After you configure a remote alert recipient, the Remote Supervisor Adapter II will send an alert to that recipient. The alert is sent through a serial connection or a network connection, a numeric pager, or an alphanumeric pager when any event selected from the Monitored Alerts group occurs. This alert contains information about the nature of the event, the time and date of the event, and the name of the system that generated the alert.

The Remote Supervisor Adapter II offers alert redundancy for several managed systems at the same location. It sends alerts only once per connection type, even when there is more than one active LAN or serial connection. However, if one connection device fails, all other interconnected devices route the alerts to the next available connection.

### Notes:

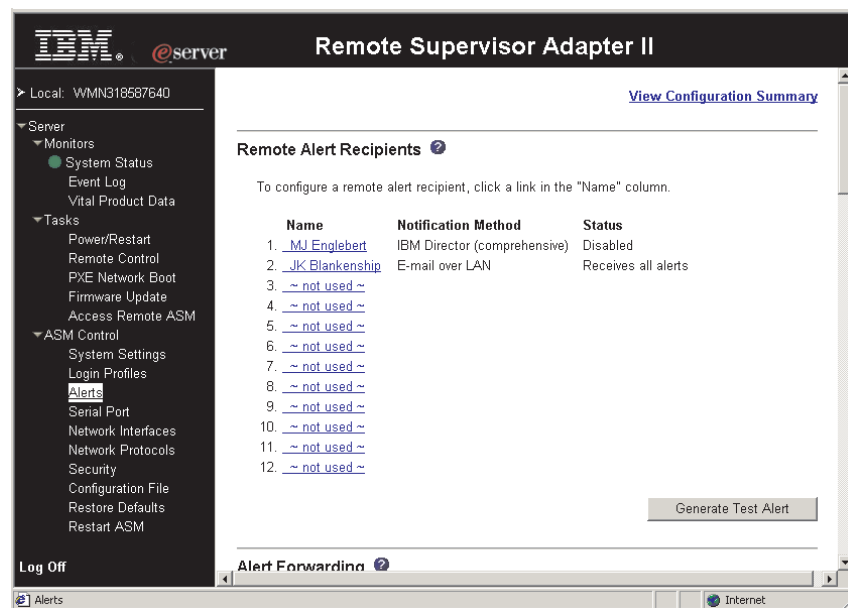
1. If the **SNMP Agent** or **SNMP Traps** fields are not set to **Enabled**, no SNMP traps are sent. For information about these fields, see “Configuring SNMP” on page 29.
2. You cannot distinguish between the alerts that are sent to remote alert recipients. All configured recipients receive each alert you select.
3. The Remote Supervisor Adapter II cannot generate alerts; it can only forward the alerts that are generated by other devices on the same ASM interconnect network.

## Configuring remote alert recipients

You can define up to 12 unique remote alert recipients. Each link for an alert recipient is labeled with the recipient name, notification method, and alert status.

Complete the following steps to configure a remote alert recipient:

1. Log in to the Remote Supervisor Adapter II for which you want to configure remote alert settings. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.
2. In the navigation pane, click **Alerts**. The Remote Alert Recipients page opens. You can see the notification method and alert status, if set, for each recipient.



3. Click one of the remote alert recipient links. An individual recipient window similar to the one in the following illustration opens.

---

**Remote Alert Recipient 2** ?

Receives critical alerts only

Status

Name

Notification method

Number

PIN

E-mail address (userid@hostname)

---

4. To have only critical alerts sent to the recipient, select the **Receives critical alerts only** check box.
5. In the **Status** field, click **Enabled** to activate the remote alert recipient.
6. In the **Name** field, type the name of the recipient or other identifier. The name you enter appears as the link for the recipient on the Alerts page.
7. In the **Notification method** field, select the notification method for reaching the recipient. Select one of the following notification methods. Not all methods are available on all servers.
  - Numeric pager
  - Alphanumeric pager
  - IBM Director over Modem
  - IBM Director over LAN
  - SNMP over LAN
  - E-mail over LAN
  - IBM Director (comprehensive)

**Note:** To configure a remote alert recipient for IBM Director over Modem, IBM Director over LAN, or IBM Director (comprehensive), the remote alert recipient must be a server with the Director Management Server installed.

8. In the **Number** field, type either the phone number, IP address, or host name at which to contact the recipient. Type a phone number if you are using one of the following notification methods:
  - Numeric pager (follow the phone number with a comma and the personal identification number [PIN])
  - Alphanumeric pager
  - IBM Director over Modem

Type an IP address or host name if you are using the IBM Director over LAN method.

9. If you chose alphanumeric pager as the notification method, in the **PIN** field, enter the PIN.
10. If you selected the E-mail over LAN notification method, in the **E-Mail address** field, type the e-mail address of the recipient.



**Note:** For the E-mail over LAN notification method to work properly, configure the Simple Mail Transfer Protocol (SMTP) options on the Network Protocols page. For more information about SMTP options, see “Configuring SMTP” on page 31.

11. Click **Save** to save your remote alert recipient profile. Repeat step 2 on page 17 through step 10 on page 18 for each remote alert recipient profile.
12. Click **Generate Test Alert** on the Remote Alert Recipients page to send a test alert to all configured remote alert recipients.

**Note:** All selected alert events are sent to all configured remote alert recipients.

## Forwarding alerts

The Alert Forwarding setting applies only to alerts forwarded from integrated system management processors (ISMPs) on an ASM interconnect network. The ISMPs on the network forward alerts only to the Remote Supervisor Adapter or Remote Supervisor Adapter II that is designated as the gateway. The gateway adapter then forwards the alerts through an Ethernet connection on the network to the alert recipients. A Remote Supervisor Adapter II is a gateway to the interconnect network if one of the following circumstances is true:

- On the Alerts Forwarding page, you click **Make this ASM the Gateway**.
- The Remote Supervisor Adapters and Remote Supervisor Adapter IIs on the network negotiate and designate the adapter to be the gateway. This occurs if none of the Remote Supervisor Adapters or Remote Supervisor Adapter IIs on the network is configured by a user to be the gateway.

### Notes:

1. There must be at least one Remote Supervisor Adapter or Remote Supervisor Adapter II on the interconnect network for ISMP alerts to be forwarded. At any time, only one Remote Supervisor Adapter or Remote Supervisor Adapter II can be the gateway on an interconnect network.
2. When Remote Supervisor Adapters and Remote Supervisor Adapter IIs are on the interconnect network, a Remote Supervisor Adapter II should be configured as the gateway.
3. When a user configures a Remote Supervisor Adapter or Remote Supervisor Adapter II to be the gateway, any existing gateway (user-defined or negotiated) ceases to be the gateway.
4. The remote alert recipients and monitored alerts for the ISMPs on the interconnect network must be configured on the gateway Remote Supervisor Adapter or Remote Supervisor Adapter II; otherwise, the alerts will not be forwarded.
5. In the event of a gateway adapter failure, a new gateway is automatically negotiated. To enable alerts to be forwarded by the negotiated gateway, you should also configure the remote alert recipients and monitored alerts on Remote Supervisor Adapters and Remote Supervisor Adapter IIs that are potential gateways.

Complete the following steps to verify whether the selected Remote Supervisor Adapter II is the gateway to the interconnect network:

1. Log in to the Remote Supervisor Adapter II for which you want to see the alert forwarding status. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.

2. In the navigation pane, click **Alerts** and scroll down to the **Alert Forwarding** section.

---

### Alert Forwarding

This setting applies only to alerts forwarded from the ISM processors on the interconnect network.

Status: Not a gateway for ISM processors

Make this ASM the Gateway

---

3. The **Status** field shows whether the Remote Supervisor Adapter II is the gateway and, if it is, whether it is a user configured or negotiated gateway. The following values are possible:
  - Not a gateway for ISMPs
  - User configured gateway for ISMPs
  - Negotiated gateway for ISMPs

## Setting remote alert attempts

The remote alert attempts settings apply only to forwarded alerts.

Complete the following steps to set the number of times the Remote Supervisor Adapter II attempts to send an alert:

1. Log in to the Remote Supervisor Adapter II on which you want to set remote alert attempts. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.
2. In the navigation pane, click **Alerts** and scroll down to the Global Remote Alert Settings section.

---

### Global Remote Alert Settings

These settings apply to all remote alert recipients.

Remote alert retry limit  times  
Delay between entries  minutes  
Delay between retries  minutes  
 Include event log with e-mail alerts

---

Use these settings to define the number of remote alert attempts and the length of time between the attempts. The settings apply to all configured remote alert recipients.

#### Remote alert retry limit

Use the **Remote alert retry limit** field to specify the number of additional times that the Remote Supervisor Adapter II will attempt to send an alert to a recipient.

#### Delay between entries

Use the **Delay between entries** field to specify the time interval (in minutes) that the Remote Supervisor Adapter II will wait before sending an alert to the next recipient in the list.

### Delay between retries

Use the **Delay between retries** field to specify the time interval (in minutes) that the Remote Supervisor Adapter II will wait between retries to send an alert to a recipient.

3. Select the **Include event log with e-mail alerts** check box to attach the local event log to all e-mail alert notifications. The event log provides a summary of the most recent events and assists with problem identification and fast recovery.

### Notes:

- a. To send the event log as an e-mail attachment, you must select E-mail over LAN as the notification method for at least one remote alert recipient.
  - b. Event logs attached in an e-mail are not forwarded to a Remote Supervisor Adapter or Remote Supervisor Adapter II on the ASM interconnect network.
4. Scroll to the bottom of the page and click **Save**.

## Setting remote alerts

Complete the following steps to select the remote alerts to be sent:

1. Log in to the Remote Supervisor Adapter II where you want to set remote alerts. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.
2. In the navigation pane, click **Alerts** and scroll down to the Monitored Alerts section.
3. Select the events you want the Remote Supervisor Adapter II to monitor.

The remote alerts are categorized by the following levels of severity:

- Critical
- Warning
- System

All alerts are stored in the event log and sent to all configured remote alert recipients.

### Critical alerts

Critical alerts are generated for events that signal that the server is no longer functioning. If the **Select all critical alerts** check box is selected, an alert can be sent for any critical alert.

Table 2. Critical remote alerts

Alphanumeric pager code	Alphanumeric recovery code	Event	Action
00	50	Temperature irregularity	Generates an alert if any of the monitored temperatures are outside critical threshold values. To view the threshold values, click the temperature readings on the System Health page. If a critical temperature condition is detected, the server shuts down and turns off, regardless of the alert notification setting.
01	51	Voltage irregularity	Generates an alert if the voltages of any of the monitored power supplies fall outside their specified operational ranges. To view the operational ranges, click the voltage readings on the System Health page. If a critical voltage condition is detected, the server shuts down and turns off, regardless of the alert notification setting.

Table 2. Critical remote alerts (continued)

Alphanumeric pager code	Alphanumeric recovery code	Event	Action
02	52	Tampering	Generates an alert if physical intrusion of the server box is detected. Tamper monitoring is not available on some servers, in which case this setting is ignored.
03	53	Multiple fan failure	Generates an alert if two or more of the cooling fans in the server fail.
04	54	Power failure	Generates an alert if any of the server power supplies fail.
05	55	Hard disk drive failure	Generates an alert if one or more of the hard disk drives in the server fail.
06	56	VRM failure	Generates an alert if one or more voltage regulator modules (VRMs) fail. This setting is ignored for servers without VRMs.
07-09			Reserved for future use.

### Warning alerts

Warning alerts are generated for events that might progress to a critical/error level. If the **Select all warning alerts** check box is selected, an alert can be sent for any warning alert.

Table 3. Warning remote alerts

Alphanumeric pager code	Alphanumeric recovery code	Event	Action
10	60	Redundant power supply failure	Generates an alert if a redundant power supply fails.
11	61	Single fan failure	Generates an alert if one fan fails.
12	62	Temperature irregularity	Generates an alert if any monitored temperatures are outside the warning threshold values. To access these temperature threshold values, click the temperature readings on the System Health page. Unlike the critical temperature event, this event will not initiate a server shutdown.
13	63	Voltage irregularity	Generates an alert if any monitored voltages are outside the warning threshold values. To access these voltage range values, click the voltage readings on the System Health page. Unlike the critical voltage event, this event will not initiate an automatic server shutdown.
14 - 19			Reserved for future use.

### System alerts

System alerts are generated for events that occur as a result of system errors. If the **Select all system alerts** check box is selected, an alert can be sent for any system alert.

#### Notes:

- a. The **Select all system alerts** check box is not available on all servers.
- b. Hard disk drive Predictive Failure Analysis<sup>®</sup> (PFA) alerts are not monitored.

Table 4. System remote alerts

Alphanumeric pager code	Alphanumeric recovery code	Event	Action
20	70	POST timeout	Generates an alert if an enabled POST timeout value is exceeded. The POST timeout value is configured in the <b>Server Timeouts</b> section on the System page.
21	71	O/S timeout	Generates an alert if an enabled operating system timeout value is exceeded. The operating system timeout value is configured in the <b>Server Timeouts</b> section on the System page. The O/S timeout alert must be checked to enable remote operating-system-failure screen capture.
22	72	Test alert	Generates an alert if the <b>Generate Test Alert</b> button is clicked on the Remote Alert Recipients page.
23	73	Power off	Generates an alert if the server is turned off.
24	74	Power on	Generates an alert if the server is turned on.
25	75	Boot failure	Generates an alert if an error occurs that prevents the server from starting.
26	76	Loader timeout	Generates an alert if an enabled server loader timeout value is exceeded. The system loader timeout value is configured in the Server Timeouts section on the System page.
27	77	PFA notification	Generates an alert if a PFA notification is generated by the server hardware. This feature is available only on servers that have PFA-enabled hardware.
28 - 29			Reserved for future use.
38	88	Partition configuration	Generates an alert if a partition configuration notification is generated by the server. This feature is available only on servers that have partitionable hardware.

4. Scroll to the bottom of the page and click **Save**.

## Setting local events

Complete the following steps to select the local events to which the Remote Supervisor Adapter II will respond:

1. Log in to the Remote Supervisor Adapter II where you want to set local events. For more information, see Chapter 2, "Opening and using the Web browser interface", on page 3.
2. In the navigation pane, click **Alerts** and scroll down to the **Monitored Local Events** section.
3. Select the events that you want to store in the event log. The Remote Supervisor Adapter II stores the notification only in the event log.

Local events are generated for events sent to IBM Director, if it is installed, on the server where the ASM subsystem is located. These events are not sent to remote alert recipients. If the **Select all local events** check box is selected, an alert can be sent for any local event.

Table 5. Local events

Event	Action
Event log 75% full	Generates a local notification if the event log reaches 75% of capacity.
Voltage irregularity	Generates a local notification if any of the monitored voltages exceed their thresholds.

Table 5. Local events (continued)

Event	Action
Power off	Generates a local notification if the server is turned off.
Power supply failure	Generates a local notification if a power supply failure is detected.
Event log full	Generates a local notification if the event log reaches its capacity. At capacity, the oldest events are deleted.
Redundant power supply failure	Generates a local notification if the redundant power supply fails.
Tampering	Generates a local notification if the server covers are removed. This feature is available only on some servers.
DASD failure	Generates a local notification if any hard disk drive failures are detected.
Remote login	Generates a local notification if a remote login occurs.
Temperature irregularity	Generates a local notification if any of the monitored temperatures exceed thresholds.
Fan failure	Generates a local notification if one or more cooling fans fail.
PFA notification	Generates a local notification if any of the hardware in the server generates a PFA event.
Partition configuration	Generates a local notification if any of the hardware in the server generates a partition configuration event.

4. Scroll to the bottom of the page and click **Save**.

---

## Configuring the serial port

The serial port on the Remote Supervisor Adapter II serves only the Remote Supervisor Adapter II and is always available for dial-out alerting purposes. You will not be able to monitor the serial port in the operating system or in any other applications.

Complete the following steps to configure your serial port:

1. Log in to the Remote Supervisor Adapter II on which you want to configure the serial port. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.
2. In the navigation pane, click **Serial Port**. A page similar to the one in the following illustration is displayed.

The screenshot shows a configuration page for 'Serial Port 1'. It includes three dropdown menus: 'Baud rate' set to 57600, 'Parity' set to NONE, and 'Stop bits' set to 1. Below these settings is a link for 'Advanced Modern Settings'.


3. In the **Baud rate** field, select the data-transfer rate.  
Use the **Baud rate** field to specify the data-transfer rate of your serial port connection. To set the baud rate, select the data-transfer rate, in bits per second, that corresponds to your serial port connection.

4. In the **Parity** field, select the error detection to be used in your serial connection.
5. In the **Stop bits** field, select the number of data-terminating 1-bits that will follow the data or any parity bit to mark the end of a transmission (normally a byte or character).

**Note:** The number of data bits is preset to 8 and cannot be changed.

6. Click **Save**.
7. If you need to set advanced settings, click **Advanced Modem Settings**. A page similar to the one in the following illustration is displayed.

---

**Port 1 Modem Settings** 

This information only needs to be modified if the alert forwarding functions are not working properly.

The strings marked with \* require a carriage return at the end (denoted ^M).

Initialization string*	<input type="text" value="ATZ^M"/>
Dial prefix string	<input type="text" value="ATDT"/>
Hangup string*	<input type="text" value="ATH0^M"/>
Dial postfix string*	<input type="text" value="^M"/>
Modem query*	<input type="text" value="AT^M"/>
Factory settings string*	<input type="text" value="AT&amp;F0^M"/>
Auto answer*	<input type="text" value="ATS0=1^M"/>
Escape string	<input type="text" value="+++"/>
Auto answer stop*	<input type="text" value="ATS0=0^M"/>
Caller ID string	<input type="text"/>
Escape guard (0 - 250)	<input type="text" value="100"/> 10ms intervals

---

Set these values only if the alert forwarding functions are not working properly. Each string marked with an asterisk (\*) must have a carriage return (^M) manually entered at the end of the field value.

The following table describes the initialization strings for this modem.

*Table 6. Port 1 settings*

Field	What you type
Initialization string*	Type the initialization string that will be used for the specified modem. A default string is provided (ATE0). Do not change this string unless your dial-out functions are not working properly.
Dial prefix string	Type the initialization string that is used before the number to be dialed. The default is ATDT.
Hangup string*	Type the initialization string that will be used to instruct the modem to disconnect. A default string is provided (ATH0). Do not change this string unless your dial-out functions are not working properly.
Dial postfix string*	Type the initialization string that is used after the number is dialed to tell the modem to stop dialing. The default is ^M.
Modem query*	Type the initialization string that is used to find out whether the modem is attached. The default is AT.

Table 6. Port 1 settings (continued)

Field	What you type
Factory settings string*	Type the initialization string that returns the modem to its factory settings when the modem is initialized. The default is AT&F0.
Auto answer*	Type the initialization string that is used to tell the modem to answer the phone when it rings. The default is to answer after one ring, ATS0=1.
Escape string	Type the initialization string that returns the modem to command mode when it is currently communicating with another modem. The default is +++.
Auto answer stop*	Type the initialization string that is used to tell the modem to stop answering the phone automatically when it rings. The default is ATS0=0.
Caller ID string	Type the initialization string that will be used to get caller ID information from the modem.
Escape guard (0 - 250)	Type the length of idle time that is used before and after the escape string is issued to the modem, so that the modem will recognize the escape string. This value is measured in 10 millisecond intervals. The default value is 1 second.

8. Click **Save**.

If you need to provide a new initialization string, see the documentation that came with your modem. Your initialization string must contain commands that configure your modem as follows:

- Command echoing OFF
- Online character echoing OFF
- Result codes ENABLED
- Verbal result codes ENABLED
- All codes and connect messages with BUSY and DT detection
- Protocol identifiers added — LAPM/MNP/NONE V42bis/MNP5
- Normal CD operations
- DTR ON-OFF hang-up, disable AA and return to command mode
- CTS hardware flow control
- RTS control of receive data to computer
- Queued and nondestructive break, no escape state

**Note:** The abbreviations in these commands have the following meanings:

<b>AA</b>	auto answer
<b>CD</b>	carrier detect
<b>CTS</b>	clear to send
<b>DT</b>	data transfer
<b>DTR</b>	data terminal ready
<b>LAPM</b>	link access protocol for modems
<b>MNP</b>	microcom networking protocol
<b>RTS</b>	ready to send

---

## Configuring an Ethernet connection to the Remote Supervisor Adapter II

On the Network Interfaces page, you can set access to the Remote Supervisor Adapter II by configuring an Ethernet connection for it.


Complete the following steps to configure the Ethernet setup for the Remote Supervisor Adapter II:



1. Log in to the Remote Supervisor Adapter II where you want to set up the configuration. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.
2. In the navigation pane, click **Network Interfaces**. A page similar to the one in the following illustration is displayed.

**Note:** The values in the following window are examples. Your settings will be different.

---

**Ethernet** 

Interface

DHCP

\*\*\* The IP configuration for this interface is assigned by a DHCP server. Follow the link \*\*\*  
 \*\*\* "IP Configuration Assigned by DHCP Server" to see the assigned configuration.

Hostname

**Static IP Configuration**

IP address

Subnet mask

Gateway address

[IP Configuration Assigned by DHCP Server](#)      [Advanced Ethernet Setup](#)

---

3. If you want to use an Ethernet connection, select **Enabled** in the **Interface** field. Ethernet is enabled by default.
4. If you want to use a Dynamic Host Configuration Protocol (DHCP) server connection, enable it by clicking either of the following choices in the DHCP field:
  - **Enabled**
  - **Try DHCP server. If it fails, use static IP config.**

The default setting is **Try DHCP server. If it fails, use static IP config.**

**Note:** Do not enable DHCP unless you have an accessible, active, and configured DHCP server on your network. When DHCP is used, the automatic configuration will override any manual settings.

If DHCP is enabled, the host name is assigned as follows:

- If the **Hostname** field contains an entry, the Remote Supervisor Adapter II DHCP support will request the DHCP server to use this host name.
- If the **Hostname** field does not contain an entry, the Remote Supervisor Adapter II DHCP support will request the DHCP server to assign a unique host name to the Remote Supervisor Adapter II.

If you enabled DHCP, go to step 12 on page 29.

If you have not enabled DHCP, continue with step 5.

5. Type the IP host name of the Remote Supervisor Adapter II in the **Hostname** field.

You can enter a maximum of 63 characters in this field, which represents the IP host name of the Remote Supervisor Adapter II. The host name defaults to ASMA, followed by the Remote Supervisor Adapter II burned-in media access control (MAC) address.

**Note:** The IP host name of the Remote Supervisor Adapter II (the **Hostname** field) and Remote Supervisor Adapter II name (the **ASM Name** field on the System page) do not automatically share the same name, because the **ASM Name** field is limited to 15 characters but the **Hostname** field can contain up to 63 characters. To minimize confusion, set the **ASM Name** field to the nonqualified portion of the IP host name. The nonqualified IP host name consists of up to the first period of a fully qualified IP host name. For example, for the fully qualified IP host name `asmcard1.us.company.com`, the nonqualified IP host name is `asmcard1`. For information about your host name, see “Setting system information” on page 10.

6. In the **IP address** field, type the IP address of the Remote Supervisor Adapter II. The IP address must contain four integers from 0 through 255 separated by periods and no spaces.
7. In the **Subnet mask** field, type the subnet mask used by the Remote Supervisor Adapter II. The subnet mask must contain four integers from 0 through 255 separated by periods and no spaces or consecutive periods. The default setting is 255.255.255.0.
8. In the **Gateway address** field, type your network gateway router. The gateway address must contain four integers from 0 through 255 separated by periods and no spaces or consecutive periods.
9. Scroll to the bottom of the page and click **Save**.
10. Click **Advanced Ethernet Setup** if you need to set additional Ethernet settings.

---

#### Advanced Ethernet Setup

Data rate	<input type="text" value="Auto"/>
Duplex	<input type="text" value="Auto"/>
Maximum transmission unit	<input type="text" value="1500"/> bytes
Locally administered MAC address	<input type="text" value="00:00:00:00:00:00"/>
Burned-in MAC address:	00:09:6B:9E:00:9D

**Note:** The burned-in MAC address takes precedence when the locally administered MAC address is set to 00:00:00:00:00:00.

---

The following table describes the functions on the Advanced Ethernet page.

*Table 7. Advanced Ethernet setup*

Field	Function
Data rate	Use the <b>Data Rate</b> field to specify the amount of data to be transferred per second over your LAN connection. To set the data rate, click the menu and select the data-transfer rate, in Mb <sup>1</sup> , that corresponds to the capability of your network. To automatically detect the data-transfer rate, select <b>Auto</b> , which is the default value.

Table 7. Advanced Ethernet setup (continued)

Field	Function
Duplex	<p>Use the <b>Duplex</b> field to specify the type of communication channel used in your network.</p> <p>To set the duplex mode, select one of the following choices:</p> <p><b>Full</b> enables data to be carried in both directions at once.</p> <p><b>Half</b> enables data to be carried in either one direction or the other, but not both at the same time.</p> <p>To automatically detect the duplex type, select <b>Auto</b>, which is the default value.</p>
Maximum transmission unit	<p>Use the <b>Maximum transmission unit</b> field to specify the maximum size of a packet (in bytes) for your network interface. For Ethernet, the valid maximum transmission unit (MTU) range is 60 - 1500. The default value for this field is 1500.</p>
Burned-in MAC address	<p>The burned-in MAC address is a unique physical address assigned to this Remote Supervisor Adapter II by the manufacturer. The address is also a read-only field.</p>
Locally administered MAC address	<p>Enter a physical address for this Remote Supervisor Adapter II in the <b>Locally administered MAC address</b> field. If a value is specified, the locally administered address overrides the burned-in MAC address. The locally administered address must be a hexadecimal value from 000000000000 through FFFFFFFF. This value must be in the form xx:xx:xx:xx:xx:xx where x is a number between 0 and 9. The Remote Supervisor Adapter II does not support the use of a multicast address. In a multicast address, the least significant bit of the first byte is set to 1. The first byte, therefore, must be an even number.</p>
<p><sup>1</sup>Mb equals approximately 1 000 000 bits.</p>	

11. Modify the advanced Ethernet settings as necessary.
12. Scroll to the bottom of the page and click **Save**.
13. Click **Back** to return to the Network Interfaces page.
14. If DHCP is enabled, the server automatically assigns the host name, IP address, gateway address, subnet mask, domain name, DHCP server IP address, and up to three DNS server IP addresses.  
To view the DHCP server assigned setting, click **IP Configuration Assigned by DHCP Server**.
15. Click **Save**.
16. In the navigation pane, click **Restart ASM** to activate the changes.

---

## Configuring network protocols

On the Network Protocols page, you can perform the following functions:

- Configure Simple Network Management Protocol (SNMP)
- Configure Domain Name System (DNS)
- Configure Simple Mail Transfer Protocol (SMTP)

### Configuring SNMP

You can query the SNMP agent to collect the sysgroup information and to send configured SNMP alerts to the configured host names or IP addresses.

**Note:** If you plan to configure Simple Network Management Protocol (SNMP) traps on the Remote Supervisor Adapter II, you must install and compile the management information base (MIB) on your SNMP manager. The MIB supports SNMP traps. The MIB is included in the Remote Supervisor Adapter II firmware update package that you downloaded from the IBM Support Web site.

Complete the following steps to configure SNMP:

1. Log in to the Remote Supervisor Adapter II where you want to configure SNMP. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.
2. In the navigation pane, click **System Settings**. In the ASM information page that opens, specify system contact and system location information. For information about the System Settings page, see “Setting system information” on page 10.
3. Scroll to the bottom of the page and click **Save**.
4. In the navigation pane, click **Network Protocols**. A page similar to the one in the following illustration is displayed.

---

**Simple Network Management Protocol (SNMP)** ⓘ

SNMP agent

SNMP traps

Community Name	Host Name or IP Address
<input type="text"/>	1. <input type="text"/>
	2. <input type="text"/>
	3. <input type="text"/>
<input type="text"/>	1. <input type="text"/>
	2. <input type="text"/>
	3. <input type="text"/>
<input type="text"/>	1. <input type="text"/>
	2. <input type="text"/>
	3. <input type="text"/>

---

5. Select **Enabled** in the **SNMP agent** and **SNMP traps** fields to forward alerts to SNMP communities on your network. To enable the SNMP agent, the following criteria must be met:
  - System contacts must be specified on the System Settings page. For information about the System Settings page settings, see “Setting system information” on page 10.
  - System location must be specified on the System Settings page.
  - At least one community name must be specified.
  - At least one valid IP address or host name (if DNS is enabled) must be specified for that community.

**Note:** Alert recipients whose notification method is SNMP will not receive alerts unless both the **SNMP agent** and the **SNMP traps** fields are set to **Enabled**.


6. Set up a community to define the administrative relationship between SNMP agents and SNMP managers. You must define at least one community. Each community definition consists of the following parameters:
  - Name
  - IP address

If either of these parameters is not correct, SNMP management access is not granted.

**Note:** If an error message window opens, make the necessary adjustments to the fields listed in the error window. Then, scroll to the bottom of the page and click **Save** to save your corrected information. You must configure at least one community to enable this SNMP agent.

7. In the **Community Name** field, enter a name or authentication string to specify the community.
8. In the corresponding **Host Name** or **IP Address** field, enter the host name or IP addresses of each community manager.
9. If a DNS server is not available on your network, scroll to the bottom of the page and click **Save**.
10. If a DNS server is available on your network, scroll to the Domain Name System (DNS) section. A page similar to the one in the following illustration is displayed.

---

**Domain Name System (DNS)** 

DNS	<input type="text" value="Enabled"/>
DNS server IP address 1	<input type="text" value="9.37.0.5"/>
DNS server IP address 2	<input type="text" value="9.37.0.6"/>
DNS server IP address 3	<input type="text" value="0.0.0.0"/>

---

11. If a DNS server (or servers) is available on your network, select **Enabled** in the **DNS** field. The **DNS** field specifies whether you use a DNS server on your network to translate host names into IP addresses.
12. If you enabled DNS, in the **DNS server IP address** fields, specify the IP addresses of up to three DNS servers on your network. Each IP address should contain integers from 0 through 255, separated by periods.
13. Scroll to the bottom of the page and click **Save**.
14. In the navigation pane, click **Restart ASM** to activate the changes.

## Configuring SMTP

Complete the following steps to specify the IP address or host name of the Simple Mail Transfer Protocol (SMTP) server.

**Note:** If you plan to set up an SMTP server for e-mail alert notifications, be sure that the name in the **Name** field in the ASM Information section of the System Settings window is valid as part of an e-mail address (for example, there are no spaces).

1. Log in to the Remote Supervisor Adapter II where you want to configure SMTP. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.

2. In the navigation pane, click **Network Protocols** and scroll down to the **SMTP** section.
3. In the **SMTP Server Host Name** or **IP Address** field, type the host name of the SMTP server. Use this field to specify the IP address or, if DNS is enabled and configured, the host name of the SMTP server.
4. Scroll to the bottom of the page and click **Save**.

---

## Using the configuration file

Select **Configuration File** in the navigation pane to:

- Back up the ASM configuration
- Restore the ASM configuration

---

### Backup ASM Configuration

To backup the configuration, click "Backup." You can [view the current configuration summary](#) before backing it up.

Backup

---

### Restore ASM Configuration

To restore the ASM configuration, select a file and click "Restore." To modify the configuration and then restore it, select a file and click "Modify & Restore."

Select configuration file to restore

Browse...

Restore

Modify and Restore

---

## Backing up your current configuration

You can download a copy of your current ASM configuration to the client computer that is running the Remote Supervisor Adapter II Web interface. Use this backup copy to restore your Remote Supervisor Adapter II configuration if it is accidentally changed or damaged. Use it as a base that you can modify to configure multiple Remote Supervisor Adapter IIs with similar configurations.

Complete the following steps to back up your current configuration:

1. Log in to the Remote Supervisor Adapter II where you want to back up your current configuration. For more information, see Chapter 2, "Opening and using the Web browser interface", on page 3.
2. In the navigation pane, click **Configuration File**.
3. In the **Backup ASM Configuration** section, click **view the current configuration summary**.
4. Verify the settings and then click **Close**.
5. To back up this configuration, click **Backup**.
6. Type a name for the backup, select the location where the file will be saved, and then click **Save**.

In Netscape Navigator, click **Save File**.

In Microsoft Internet Explorer, select **Save this file to disk**, and then click **OK**.

## Restoring and modifying your ASM configuration

You can restore a saved configuration in full, or you can modify key fields in the saved configuration before restoring the configuration to your Remote Supervisor Adapter II. Modifying the configuration file before restoring it helps you set up multiple Remote Supervisor Adapter IIs with similar configurations. You can quickly specify parameters that require unique values such as names and IP addresses, without having to enter common, shared information.

Complete the following steps to restore or modify your current configuration:

1. Log in to the Remote Supervisor Adapter II where you want to restore the configuration. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.
2. In the navigation pane, click **Configuration File**.
3. In the Restore ASM Configuration section, click **Browse**.
4. Click the configuration file that you want; then, click **Open**. The file (including the full path) appears in the box beside **Browse**.
5. If you do not want to make changes to the configuration file, click **Restore**. A new window opens with the ASM configuration information. Verify that this is the configuration that you want to restore. If it is not the correct configuration, click **Cancel**.

If you want to make changes to the configuration file before restoring, click **Modify and Restore** to open an editable configuration summary window. Initially, only the fields that allow changes appear. To change between this view and the complete configuration summary view, click the **Toggle View** button at the top or bottom of the window. To modify the contents of a field, click the corresponding text box and enter the data.

**Note:** When you click **Restore** or **Modify and Restore**, an alert window might open if the configuration file you are attempting to restore was created by a different type of service processor or was created by the same type of service processor with older firmware (and therefore, less functionality). This alert message will include a list of system-management functions that you will have to configure manually after the restoration is complete. Some functions require configurations on more than one window.

6. To proceed with restoring this file to the Remote Supervisor Adapter II, click **Restore Configuration**. A progress indicator appears as the firmware on the Remote Supervisor Adapter II is updated. A confirmation window opens to verify whether the update was successful.
7. After receiving a confirmation that the restore process is complete, in the navigation pane, click **Restart ASM**; then, click **Restart**.
8. Click **OK** to confirm that you want to restart your Remote Supervisor Adapter II.
9. Click **OK** to close the current browser window.
10. To log in to the Remote Supervisor Adapter II again, start your browser, and follow your regular login process.

---

## Restoring ASM defaults

Use the **Restore Defaults** link to restore the default configuration of the Remote Supervisor Adapter II, if you have read/write access.

**Attention:** When you click **Restore Defaults**, you will lose all the modifications you made to the Remote Supervisor Adapter II. You also will lose the remote control of the remote servers.

Complete the following steps to restore the ASM defaults:

1. Log in to the Remote Supervisor Adapter II. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.
2. In the navigation pane, click **Restore Defaults** to restore default settings of the Remote Supervisor Adapter II. If this is a local system, you will lose your TCP/IP connection, and you must reconfigure the network interface to restore connectivity.
3. Log in again to use the Remote Supervisor Adapter II Web interface.
4. Reconfigure the network interface to restore connectivity. For information about the network interface, see “Configuring an Ethernet connection to the Remote Supervisor Adapter II” on page 26.

---

## Restarting ASM

Use the **Restart ASM** link to restart the Remote Supervisor Adapter II. You can perform this function only if you have read/write access. Any TCP/IP, modem, or interconnect connections are temporarily dropped. You must log in again to use the Remote Supervisor Adapter II Web interface.

Complete the following steps to restart the Remote Supervisor Adapter II or ISMP:

1. In the navigation pane, click **Restart ASM** to restart a Remote Supervisor Adapter II or ISMP. Your TCP/IP or modem connections are lost.
2. Log in again to use the Remote Supervisor Adapter II Web interface.

---

## Logging off

Complete the following steps to log off the Remote Supervisor Adapter II or another remote server:

1. In the navigation pane, click **Log Off**.

**Note:** If you are logged in to another remote server, you must first select **Log Off Remote ASM**.

2. If you are running Internet Explorer or Netscape Navigator, click **Yes** in the confirmation window.

The current browser window closes to maintain security. You must manually close other open browser windows, if any, to prevent a cached version of your user ID and password from remaining available.



## Chapter 4. Monitoring remote server status

Use the links under the Monitors heading of the navigation pane to view the status of the server you are accessing.

From the System Status pages, you can:

- Monitor the power status of the server and view the state of the operating system
- View the server temperature readings, voltage thresholds, and fan speeds
- View the latest server operating-system-failure screen capture
- View the list of users logged in to the Remote Supervisor Adapter II

From the Event Log page, you can:

- View certain Advanced System Management events recorded in the event log of the Remote Supervisor Adapter II
- View the severity of events

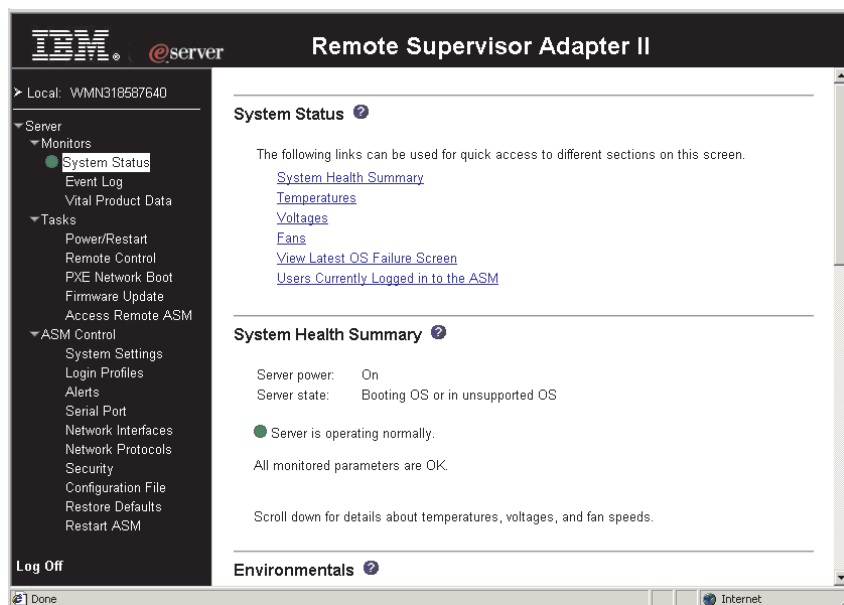
From the Vital Product Data (VPD) page, you can view the vital product data of the Remote Supervisor Adapter II, the server in which it is installed, and the ISMP.

### Viewing system health

On the System Health Summary page, you can monitor the temperature readings, voltage thresholds, and fan status of your server.

Complete the following steps to view the system health and environmental information of the server:

1. Log in to the Remote Supervisor Adapter II. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.
2. In the navigation pane, click **System Health** to view a dynamically-generated update on the overall health of the server. A page similar to the one in the following illustration is displayed.



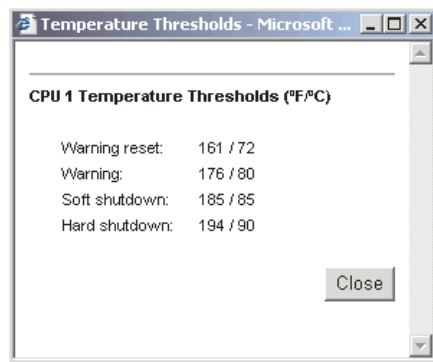
The status of your server determines the message shown at the top of the System Health Summary page. One of the following symbols appears:

- A solid green circle and the phrase Server is operating normally
- Either a red circle containing an X or a yellow triangle containing an exclamation point and the phrase One or more monitored parameters are abnormal

If the monitored parameters are operating outside normal ranges, a list of the specific abnormal parameters is displayed on the System Health Summary page.

3. Scroll down to the **Temperatures** section. The Remote Supervisor Adapter II tracks the current temperature readings and threshold levels for system components such as microprocessors, system board, and hard disk drive backplane.

When you click a temperature reading, a window similar to the one in the following illustration opens.



The Temperature Thresholds page displays the temperature levels at which the Remote Supervisor Adapter II reacts. The temperature threshold values are preset on the remote server and cannot be changed.

The reported temperatures for the CPU, hard disk drive, and system are measured against the following threshold ranges:

#### **Warning Reset**

If a warning was sent and the temperature returns to any value below the warning reset value, the server assumes the temperature has returned to normal and no further alerts are generated.

#### **Warning**

When the temperature reaches a specified value, a temperature alert is sent to configured remote alert recipients. You must select the **Temperature** check box on the Alerts page for the alert to be sent.

For more information about selecting Alert options, see "Setting remote alerts" on page 21.

#### **Soft Shutdown**

When the temperature reaches a specified value higher than the warning value (the soft shutdown threshold), a second temperature alert is sent to configured remote alert recipients, and the server begins the shutdown process with an orderly operating-system shutdown. The server then turns itself off. You must select the **Temperature** check box on the Alerts page for the alert to be sent.

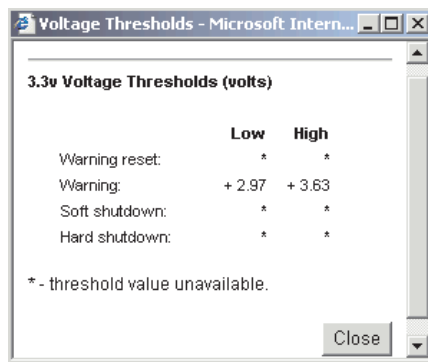
### Hard Shutdown

When the temperature reaches a specified value higher than the soft shutdown value (the hard shutdown threshold), the server immediately shuts down and sends an alert to configured remote alert recipients. You must select the **Temperature** check box on the Alerts page for the alert to be sent.

**Note:** The hard shutdown alert is sent only if a soft shutdown alert has not yet been sent.

4. Scroll down to the **Voltages** section. The Remote Supervisor Adapter II will send an alert if any monitored power source voltage falls outside its specified operational ranges.

If you click a voltage reading, a window similar to the one in the following illustration opens.



The Voltage Thresholds page displays the voltage ranges at which the Remote Supervisor Adapter II reacts. The voltage threshold values are preset on the remote server and cannot be changed.

The Remote Supervisor Adapter II Web interface displays the voltage readings of the system board and the voltage regulator modules (VRM). The system sets a voltage range at which the following actions are taken:

### Warning Reset

When the voltage drops below or exceeds the warning voltage range and then recovers to that range, the server assumes the voltage has returned to normal and no further alerts are generated.

### Warning

When the voltage drops below or exceeds a specified voltage range, a voltage alert is sent to configured remote alert recipients. You must select the **Voltage** check box on the Alerts page for the alert to be sent.

### Soft Shutdown

When the voltage drops below or exceeds a specified voltage range, a voltage alert is sent to configured remote alert recipients, and the server begins the shutdown process with an orderly operating-system shutdown. The server then turns itself off. You must select the **Voltage** check box on the Alerts page for the alert to be sent.

### Hard Shutdown

When the voltage drops below or exceeds a specified voltage range, the server immediately shuts down and sends an alert to configured remote alert recipients. You must select the **Voltage** check box on the Alerts page for the alert to be sent.

**Note:** The hard shutdown alert is sent only if a soft shutdown alert has not yet been sent.

5. Scroll down to the **Fan Speeds** section. The Remote Supervisor Adapter II Web interface displays the running speed of the server fans (expressed in a percentage of the maximum fan speed). You receive a fan alert (Multiple Fan Failure or Single Fan Failure) when the fan speeds drop to an unacceptable level or the fans stop. You must select the **Fan** check box on the Alerts page for the alert to be sent.
6. Scroll down to the **Display Latest OS Failure Screen** section. Click **View OS Failure Screen** to access an image of the operating-system-failure screen captured when the server stopped functioning.

**Notes:**

- a. To capture operating-system-failure screens, you must enable the OS Watchdog feature as described in “Setting server timeouts” on page 11.
- b. The operating-system-failure screen capture is available only if a supported operating system is installed on the server.

If an operating-system-failure screen event occurs while the operating system is running but then the server operating system stops running, the operating-system timeout is triggered, which causes the Remote Supervisor Adapter II to capture the operating-system-failure screen data and store it. The operating-system-failure screen image shows the date and time of the capture. The image will not be overwritten during the next operating-system installation because the Remote Supervisor Adapter II does not capture the operating-system loader screen. Only error conditions are captured and maintained. The Remote Supervisor Adapter II stores only the most recent error event information, overwriting older information when a new error event occurs.

Complete the following steps to remotely access a server operating-system-failure screen image:

- a. Log in to the Remote Supervisor Adapter. For more information, see Chapter 2, “Opening and using the ASM Web interface” on page 3.
  - b. In the navigation pane, click **System Health**, and then scroll down to the **Display Latest OS Failure Screen** section.
  - c. Click **View OS Failure Screen**. The operating-system-failure screen image is displayed on your screen.
7. Scroll down to the **Users Currently Logged in** section. The Remote Supervisor Adapter II Web interface displays the login ID and access method of each user logged in to the Remote Supervisor Adapter II.

---

**Users Currently Logged in to WMN318587640** ⓘ

Currently 2 user(s) are logged in to WMN318587640.

Login ID	Access Method
USERID	Web browser
Logmein	Web browser

---

## Viewing the event log

The Event Log page contains all entries that are currently stored in the server event log and POST event log of the remote managed server. Information about all remote access attempts is recorded in the Remote Supervisor Adapter II event log. You can view the event log for all of the servers on an ASM interconnect network. The Remote Supervisor Adapter II time stamps all events and logs them into the event log, sending out the following alerts, if configured to do so by the system administrator:

- Event log 75% full
- Event log full

The event log has a limited capacity. When that limit is reached, the older events are deleted in a first-in, first-out order.

You can sort and filter entries in the event log.

Complete the following steps to access and view the event log:

1. Log in to the Remote Supervisor Adapter II. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.
2. In the navigation pane, click **Event Log** to view the recent history of events on the server. A page similar to the one in the following illustration is displayed.

The screenshot shows the 'Remote Supervisor Adapter II' web interface. The left navigation pane is expanded to 'Event Log'. The main content area is titled 'Event Log' and contains a legend for severity levels: Error (E), Warning (W), and Info (I). Below the legend is a table of event log entries. The table has columns for Index, Sev, Source, Date/Time, and Text. The entries are as follows:

Index	Sev	Source	Date/Time	Text
1	I	POSTBIOS	02/24/03, 16:43:40	Planar video disabled due to add-in video card
2	E	SERVPROC	02/24/03, 16:43:11	Environmental Monitor not responding.
3	E	POSTBIOS	02/24/03, 16:43:09	178 System-security error--VPD not available
4	I	SERVPROC	02/24/03, 16:41:50	System Complex Powered Down
5	I	SERVPROC	02/24/03, 16:41:36	System log cleared.

Below the table, it says 'End of Log.' At the bottom of the interface, there are three buttons: 'Reload Log', 'Clear Log', and 'Save Log as Text File'.

3. Scroll down to view the complete contents of the event log. The events are given the following levels of severity:

### Informational

This severity level is assigned to an event of which you should take note.

### Warning

This severity level is assigned to an event that could affect server performance.

**Error** This severity level is assigned to an event that needs immediate attention.

The Remote Supervisor Adapter II Web interface distinguishes warning events with the letter W on a yellow background in the severity column and error events with the letter E on a red background.

Severity	Source	Date	
E	Error	POSTBIOS	Filter Disable Filter
W	Warning	SERVPROC	
I	Info		

4. Click **Save Log as Text File** to save the contents of the event log as a text file. Click **Reload Log** to refresh the display of the event log. Click **Clear Log** to delete the contents of the event log.

## Viewing vital product data

When the server starts, the Remote Supervisor Adapter II collects system, basic input/output (BIOS) information, and server component vital product data (VPD) and stores it in nonvolatile memory. You can access this information at any time from almost any computer. The Vital Product Data page contains key information about the remote managed server that the Remote Supervisor Adapter II is monitoring.

Complete the following steps to view the server component vital product data:

1. Log in to the Remote Supervisor Adapter II. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.
2. In the navigation pane, click **Vital Product Data** to view the status of the hardware and software components on the server.
3. Scroll down to view the following VPD readings:

### Machine level VPD

The vital product data for the server appears in this section. For viewing VPD, the machine-level VPD includes a universal unique identifier (UUID).

**Note:** The machine-level VPD, component-level VPD, and component activity log provide information only when the server is turned on.

Table 8. Machine-level vital product data

Field	Function
Machine type	Identifies the type of server the Remote Supervisor Adapter II is monitoring.
Machine model	Identifies the model number of the server the Remote Supervisor Adapter II is monitoring.
Serial number	Identifies the serial number of the server the Remote Supervisor Adapter II is monitoring.
UUID	Identifies the universal unique identifier (UUID), a 32-digit hexadecimal number, of the server that the Remote Supervisor Adapter II is monitoring.

### Component level VPD

The vital product data for the components of the remote managed server appears in this section.

Table 9. Component-level vital product data

Field	Function
FRU number	Identifies the field replaceable unit (FRU) number (a seven-digit alphanumeric identifier) for each component.
Serial number	Identifies the serial number of each component.
Mfg ID	Identifies the manufacturer ID for each component.
Slot	Identifies the slot number where the component is located.

### Component Activity Log

You can find a record of component activity in this section.

Table 10. Component activity log

Field	Function
FRU number	Identifies the field replaceable unit (FRU) number (a seven-digit alphanumeric identifier) of the component.
Serial number	Identifies the serial number of the component.
Manufacturer ID	Identifies the manufacturer of the component.
Slot	Identifies the slot number where the component is located.
Action	Identifies the action taken by each component.
Timestamp	Identifies the date and time of the component action. The date is displayed in the MM/DD/YY format. The time is displayed in the HH:MM:SS format.

In addition, the component activity log tracks the following server components:

- Power supplies
- DIMMs
- CPUs
- System board
- Power backplane

### POST/BIOS VPD

You can find the power-on self-test (POST) or basic input/output system (BIOS) firmware code VPD for the remote managed server in this section.

Table 11. POST/BIOS vital product data

Field	Function
Version	Indicates the version number of the POST/BIOS code.
Build level	Indicates the level of the POST/BIOS code.
Build date	Indicates when the POST/BIOS code was built.

### Diagnostics VPD

You can find the diagnostic code VPD for the remote managed server in this section.

Table 12. Diagnostics vital product data

Field	Function
Version	Indicates the version number of the diagnostic code.

Table 12. Diagnostics vital product data (continued)

Field	Function
Build level	Indicates the level of the diagnostic code.
Build date	Indicates when the diagnostic code was built.

### ASM VPD

You can find vital product data for the Remote Supervisor Adapter II in this section.

Table 13. ASM vital product data

Field	Function
Firmware type	Identifies the ASM firmware component type: main application, boot ROM, or video BIOS.
Build ID	Identifies the build IDs of the application firmware and the startup ROM firmware.
File name	Identifies the file names of the application firmware and the startup ROM firmware.
Release date	Identifies the release dates of the application firmware and the startup ROM firmware.
Revision	Identifies the revision numbers of the application firmware and the startup ROM firmware.

### Integrated system management processor VPD

You can find the vital product data for the integrated system management processor (ISMP) firmware code in this section.

Table 14. Integrated system management processor vital product data

Field	Function
Firmware revision	Identifies the revision number of the integrated system management processor firmware.



## Chapter 5. Performing Remote Supervisor Adapter II tasks

Use the functions under the Tasks heading in the navigation pane to directly control the actions of the Remote Supervisor Adapter II and your server. The tasks you can perform depend on the server in which the Remote Supervisor Adapter II is installed.

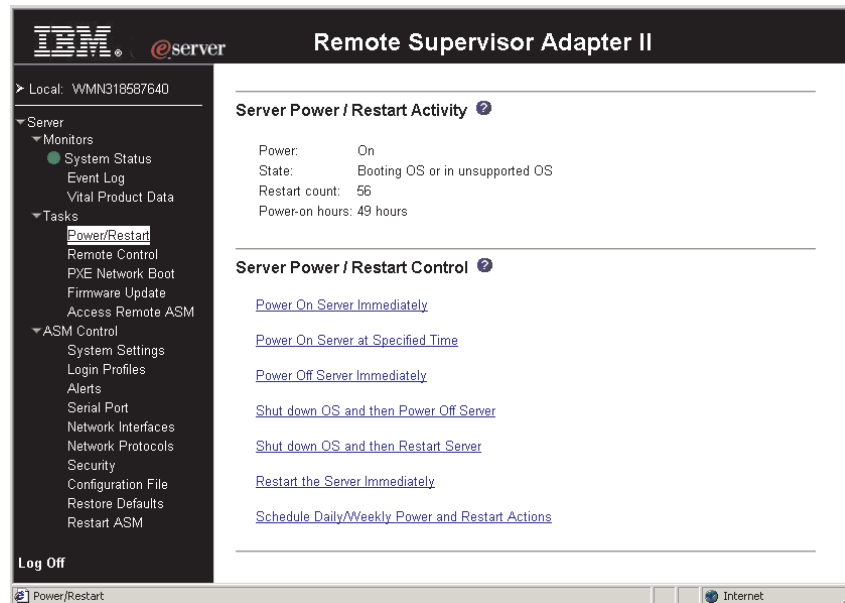
You can perform the following tasks:

- View server power and restart activity
- Remotely control the power status of the server
- Remotely access the server console
- Remotely attach a disk or disk image to the server
- Update the Remote Supervisor Adapter II firmware
- Access other Remote Supervisor Adapter IIs and Remote Supervisor Adapters

**Note:** Some features are available only on servers running a supported Microsoft Windows operating system.

### Server power and restart activity

The Server Power and Restart Activity section displays the power status of the server when the Web page was generated.



**Power** The **Power** field shows the power status of the server at the time this Web page was generated.

**State** The **State** field shows the state of the server when this Web page was generated. The following states are possible:

- System power off/State unknown
- In POST
- Stopped in POST (Error detected)
- Booted Flash or System partition

- Booting OS or in unsupported OS (could be in the operating system if the operating system or application does not report the new system state)
- In OS
- CPUs held in reset
- System power on/Before POST

#### **Restart count**

The **Restart count** field shows the number of times the server has been restarted.

**Note:** The counter is reset to zero each time the ASM subsystem is cleared to factory defaults.

#### **Power-on hours**

The **Power-on hours** field shows the total number of hours the server has been turned on.

---

## **Remotely controlling the power status of a server**

The Remote Supervisor Adapter II provides full remote power control over your server with power-on, power-off, and restart actions. In addition, power-on and restart statistics are captured and displayed to show server hardware availability.

**Attention:** Read the following information to prevent the loss of data or damage to data when you perform a remote shutdown of your operating system:

- If the Windows 2000, Red Hat Linux, or SuSE Linux operating system is installed on your server, you need to install only the Remote Supervisor Adapter II device driver to support remote operating system shutdown.
- In the **Power off delay** field, if the value is less than 45 seconds, the device driver will adjust the value to 45 seconds when the device driver loads. You can decrease the power-off delay value after the server has started, but the device driver will reset it to 45 seconds on the next server restart. The device driver will not change a power-off delay value that is 45 seconds or greater.

To perform the actions in the **Server Power/Restart Control** section, you must have read/write access to the Remote Supervisor Adapter II. For the operating system shutdown options, the Remote Supervisor Adapter II communicates with the system-management software through the device driver and the system-management software initiates the shutdown.

Complete the following steps to perform server power and restart actions.

**Note:** Select the following options only in case of an emergency, or if you are offsite and the server is nonresponsive.

1. Log in to the Remote Supervisor Adapter II. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.
2. In the navigation pane, click **Power/Restart**. Scroll down to the **Server Power/Restart Control** section.
3. Click one of the following options:

#### **Power on server immediately**

To turn on this server and start the operating system, click **Power On Server Immediately**.

**Power on server at specified time**

To turn on this server at a specified time and start the operating system, click **Power on Server at Specified Time** and set the time to turn on the server.

**Power off server immediately**

To turn off this server without shutting down the operating system, click **Power Off Server Immediately**.

**Shut down OS and then power off server**

To shut down the operating system and then turn off this server, click **Shutdown OS and then Power Off Server**. This option requires that the Remote Supervisor Adapter II device driver is installed. You might also need to install IBM Director Agent.

**Shut down OS and then restart server**

To restart the operating system, click **Shut down OS and then Restart Server**. This option requires that the Remote Supervisor Adapter II device driver is installed. You might also need to install IBM Director Agent.

**Restart the server immediately**

To turn off and then turn on this server immediately without first shutting down the operating system, click **Restart the Server Immediately**.

**Schedule Daily/Weekly Power and Restart Actions**

To shut down the operating system, turn off the server at a specified daily or weekly time (with or without restarting the server), and turn on the server at a specified daily or weekly time, click **Schedule Daily/Weekly Power and Restart Actions**.

A confirmation message is displayed if you select any of these options, and you can cancel the operation if it was selected accidentally.

---

## Remote control

When you use the remote control function, you can view and interact with the server console, and you can assign to the server a CD-ROM drive, diskette drive, or disk image that is on your computer.

You must log in to the Remote Supervisor Adapter II with a user ID that has read/write access to use any of the remote control features.

## Remote console

A remote console is an interactive graphical user interface (GUI) display of the server, viewed on your computer. You see on your monitor exactly what is on the server console, and you have keyboard and mouse control of the console.

Complete the following steps to remotely access a server console:

1. Log in to the Remote Supervisor Adapter II. For more information, see Chapter 2, "Opening and using the Web browser interface", on page 3.
2. In the navigation pane, click **Remote Control**.
3. In the Remote Control page, click **Start Remote Control**. A separate Remote Control window opens that displays the server console in the Remote Console area. The Remote Control window also contains the remote disk function in the Remote Disk area.

**Notes:**

- a. Remote console keyboard support includes all keys. Icons are provided for keys that might have a special meaning to your computer. For example, to transmit Ctrl+Alt+Del to the server, you must click the **Ctrl** icon and then press the Alt and Del keys on the keyboard.
  - b. If you have mouse or keyboard problems when using Remote Control, see the help available from the Remote Control page in the Web interface.
  - c. If you use the remote console to change settings for the Remote Supervisor Adapter II in the server Configuration/Setup Utility program (**Advanced Setup→RSA II Settings**), the server restarts the adapter and you lose the remote console and the login session. After a short delay, you can log in to the adapter again with a new session, start the remote console again, and exit the server Configuration/Setup Utility program.
4. If the server is running the Microsoft Windows operating system and a Microsoft Windows logon window opens, click the **Ctrl** icon, and then press Alt+Del on your keyboard to proceed. If the remote Windows desktop is already displayed, use the mouse or the keyboard to navigate.

You can close the Remote Control window to disconnect from viewing the server console.

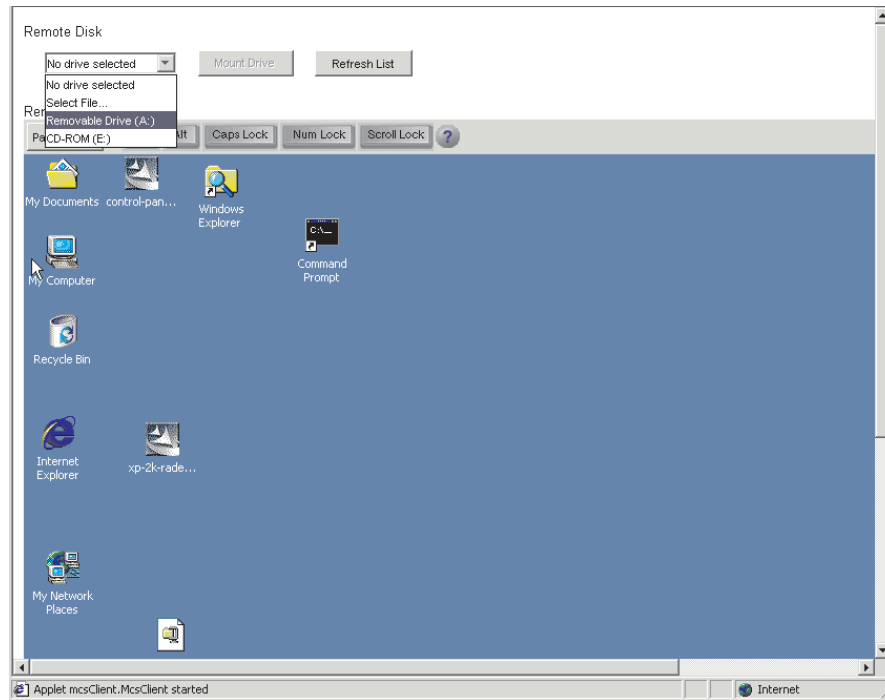
**Note:** Do not close the Remote Control window if a remote disk is currently mounted. See step 6 on page 47 for instructions for closing and unmounting a remote disk.

## Remote disk

From the Remote Control window, you can assign to the server a CD-ROM drive or diskette drive that is on your computer, or you can specify a disk image on your computer for the server to use. You can use the drive for functions such as restarting (booting) the server, updating BIOS code or diagnostics code, installing new software on the server, and installing or updating the operating system on the server. You can use the Remote Console function to access the remote disk. The drive will appear as a USB drive on the server.

**Notes:**

1. The remote disk is not recognized by the Linux operating system on a server. You can use the remote disk for functions on that server that do not require the server operating system, such as restarting from the remote disk or updating the server firmware.
2. The remote disk function requires the following software:
  - Server (for the server operating system to support the remote disk): Microsoft Windows 2000 with Service Pack 3 or later.
  - Client: Microsoft Windows 2000 or later and the Java 1.4 Plug-in or later.
3. The client system must have an Intel Pentium® III microprocessor or greater, operating at 700 MHz or faster, or equivalent.



Complete the following steps to assign a disk drive or disk image on your computer to the server:

1. Log in to the Remote Supervisor Adapter II. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.
2. In the navigation pane, click **Remote Control**.
3. In the Remote Control page, click **Start Remote Control**. A separate Remote Control window opens that displays the remote disk controls in the **Remote Disk** area. The Remote Control window also contains the server console in the **Remote Console** area (see “Remote console” on page 45).
4. In the drop-down list in the **Remote Disk** section of the Remote Control window, click the item you want. The choices are listed by the type of drive, followed by volume label.

#### Select File

A disk image on your computer.

#### Removable Drive

A diskette drive on your computer.

#### CD-ROM

A CD-ROM drive on your computer.

5. Click **Mount Drive**. If you clicked **Select File** in step 4, browse to select the disk image file to use.  
The drive or disk image will function as a USB device connected to the server.  
To refresh the list of available drives on your computer, click **Refresh List** in the Remote Control window.
6. When you have finished using the drive or disk image, close and unmount it. For Microsoft Windows, complete the following steps to close and unmount the drive or drive image.
  - a. Double-click the **Unplug or Eject Hardware** icon in the Windows taskbar at the bottom right of the screen. If there is no icon, complete the following steps:

- 1) In the Microsoft Windows Control Panel, click **Add/Remove Hardware**; then, click **Next**.
  - 2) Select **Uninstall/Unplug a device**; then, click **Next**.
  - 3) Click **Unplug/Eject a device**; then, click **Next**.
  - 4) Continue to the next step.
- b. Select **USB Mass Storage Device** and click **Stop**.
  - c. Click **Close**.
  - d. In the Remote Control window, click **Unmount Drive**.

---

## Updating firmware

Use the Firmware Update option on the navigation pane to update the firmware of the Remote Supervisor Adapter II.

**Note:** To update remotely the firmware or operating system on the server, see “Remote disk” on page 46.

Complete the following steps to update the startup or main application files of your Remote Supervisor Adapter II:

1. Log in to the Remote Supervisor Adapter II. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.
2. In the navigation pane, click **Firmware Update**.
3. Click **Browse**.
4. Navigate to the PKT or PKC file you want to update.

**Note:** When you transfer (or flash) the main application packet, you must also flash the remote graphics packet separately.

5. Click **Open**.  
The file (including the full path) appears in the box beside **Browse**.
6. To begin the update process, click **Update**.  
A progress indicator opens as the file is transferred to temporary storage on the Remote Supervisor Adapter II. A confirmation window opens when the file transfer is completed.
7. Verify that the PKT or PKC file shown on the Confirm Firmware Update window is what you intend to update. If it is not, click **Cancel**.
8. To complete the update process, click **Continue**.  
A progress indicator opens as the firmware on the Remote Supervisor Adapter II is flashed. A confirmation window opens to verify that the update was successful.
9. After receiving a confirmation that the update process is completed, go to the Restart ASM window and click **Restart**.
10. Click **OK** to confirm that you want to restart the Remote Supervisor Adapter II.
11. Click **OK** to close the current browser window.
12. To log in to the Remote Supervisor Adapter II again, start your browser, and follow your regular login process.

**Note:** To cancel this process, click **Cancel**.

---

## Accessing remote adapters through an ASM interconnect network

You can connect to remote systems through the ASM interconnect network from the Access Remote ASM link. The Remote ASM Access table displays color-coded icons to indicate the overall status of each remote system in the System Health column. The system name is the name corresponding to each remote system. The ASM Interconnect Connection column provides a login link that you can use to quickly access each remote system.

**Note:** Although it is possible to access a Remote Supervisor Adapter II from a server that is using a Remote Supervisor Adapter, doing so does not present the full function of a Remote Supervisor Adapter II. You should log in to the Remote Supervisor Adapter II first, then log in to the Remote Supervisor Adapter, to obtain full Remote Supervisor Adapter II functionality.

Complete the following steps to access a Remote Supervisor Adapter, a Remote Supervisor Adapter II, an ASM PCI adapter, or an ASM processor on the ASM interconnect network:

1. Log in to the Remote Supervisor Adapter II. For more information, see Chapter 2, “Opening and using the Web browser interface”, on page 3.
2. In the navigation pane, click **Access Remote ASM**. A page similar to the one in the following illustration is displayed.

---

### Remote ASM Access

System Health	ASM Name	ASM Interconnect Connection	Direct LAN Connection
	WEBSERVER	<a href="#">login</a>	<a href="#">9.37.112.235</a>

Click on "login" to establish a session with a specified ASM.

Click on the IP address to start a direct LAN session in a new browser window.

---

3. The Remote ASM Access page contains a table that lists processors and adapters linked to the host server. The table also displays the following information:

#### System Health

The system health icon of the remote service processor is displayed in this column.

#### ASM Name

The name of the remote service processor is displayed in this column.

#### ASM Interconnect Connection

The ASM Interconnect Connection column provides a login link that you can use to quickly access each remote system through the ASM interconnect network. To log in to a remote system displayed in the table, click the login link corresponding to the remote system that you want to access. Then, follow the standard login procedure to gain access to that system.

#### Direct LAN Connection

Click the IP address link to bypass the ASM interconnect connection and to connect to a remote system directly through your Ethernet network. This connection offers faster access to a remote ASM.

To directly log in to a remote system displayed in the table, click the IP address link corresponding to the remote system that you want to access. Then, follow the standard login procedure to gain access to that remote system.

**Note:** In certain cases, no IP address link for a direct LAN connection will be available, for one of the following reasons:

**no LAN support**

The service processor of the remote system does not have access to a LAN port.

**function not supported**

The service processor of the remote system does not have the ability to report its IP address through the ASM interconnect network.

**no LAN connection**

The service processor of the remote system has one of the following conditions:

- It has not been manually configured with an IP address.
- It failed to receive a dynamic IP address assignment from a DHCP server.
- It has a faulty physical LAN connection.

4. Click the **login** link that corresponds to the processor or adapter that you want to access under the ASM Interconnect Connection column heading.

**Note:** It might take up to 45 seconds for newly attached servers to be reflected in the table of available remote servers, and up to 2 minutes for servers to be removed from the table when detached from the ASM interconnect network.

The Enter Network Password window opens.

5. Type your user name and password and click **OK**. The System Health Summary page opens. The adapter or processor name appears in orange above the navigation pane.

**Note:** Depending on the service processor that is on the remote server, some options might not be available.

6. Click **Log Off Remote ASM** to log off of the remote server.



---

## Appendix A. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This appendix contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your xSeries or IntelliStation® system, and whom to call for service, if it is necessary.

---

### Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system is turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system.
- Go to the IBM Support Web site at <http://www.ibm.com/pc/support/> to check for technical information, hints, tips, and new device drivers.
- Use an IBM discussion forum on the IBM Web site to ask questions.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the publications that are provided with your system and software. The information that comes with your system also describes the diagnostic tests that you can perform. Most xSeries and IntelliStation systems, operating systems, and programs come with information that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the information for the operating system or program.

---

### Using the documentation

Information about your IBM xSeries or IntelliStation system and preinstalled software, if any, is available in the documentation that comes with your system. That documentation includes printed books, online books, readme files, and help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to <http://www.ibm.com/pc/support/> and follow the instructions. Also, you can order publications through the IBM Publications Ordering System at <http://www.elink.ibm.com/public/applications/publications/cgibin/pbi.cgi>.

---

### Getting help and information from the World Wide Web

On the World Wide Web, the IBM Web site has up-to-date information about IBM xSeries and IntelliStation products, services, and support. The address for IBM xSeries information is <http://www.ibm.com/eserver/xseries/>. The address for IBM IntelliStation information is <http://www.ibm.com/pc/intellistation/>.

You can find service information for your IBM products, including supported options, at <http://www.ibm.com/pc/support/>.

---

## **Software service and support**

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with xSeries servers, IntelliStation workstations, and appliances. For information about which products are supported by Support Line in your country or region, go to <http://www.ibm.com/services/sl/products/>.

For more information about Support Line and other IBM services, go to <http://www.ibm.com/services/>, or go to <http://www.ibm.com/planetwide/> for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

---

## **Hardware service and support**

You can receive hardware service through IBM Integrated Technology Services or through your IBM reseller, if your reseller is authorized by IBM to provide warranty service. Go to <http://www.ibm.com/planetwide/> for support telephone numbers, or in the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

---

## Appendix B. Notices

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

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

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

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.*

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product, and use of those Web sites is at your own risk.

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

---

### Edition notice

**© Copyright International Business Machines Corporation 2003. All rights reserved.**

U.S. Government Users Restricted Rights — Use, duplication, or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

## Trademarks

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

e-business logo

@server

IBM

IntelliStation

Predictive Failure  
Analysis

ServerGuide

ServerProven

xSeries

Lotus, Lotus Notes, SmartSuite, and Domino are trademarks of Lotus Development Corporation and/or IBM Corporation in the United States, other countries, or both.

ActionMedia, LANDesk, MMX, Pentium, and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

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

---

# Index

## A

- alerts
  - configuring recipients for 17
  - forwarding from ISMP 19
  - gateway (forwarding) 19
  - ISMP, gateway to network 19
  - selecting to send
    - critical 21
    - system 22
    - warning 22
  - setting remote attempts 20
- alphanumeric pager codes
  - critical alerts 21
  - system alerts 22
  - warning alerts 22
- ASM configuration
  - backing up 32
  - modifying and restoring 33
- ASM defaults, restoring 33
- ASM interconnect network
  - accessing remote adapters 49
  - forwarding ISMP alerts 19
- ASM vital product data, viewing 42
- ASM Web interface, opening and using 3

## B

- backing up ASM configuration 32
- browser, Web requirements 2

## C

- changing the host server startup sequence 5
- component activity log vital product data, viewing 41
- component level vital product data, viewing 40
- configuring
  - DNS 31
  - Ethernet connection 26
  - remote alert recipients 17
  - SMTP 31
  - SNMP 29
- critical alerts 21

## D

- daylight saving time, adjusting for 14
- defaults, restoring configuration 33
- diagnostic code vital product data, viewing 41
- disk, remote 46
- DNS, configuring 31

## E

- Ethernet connection, configuring 26
- event log
  - severity levels 39

- event log (*continued*)
  - viewing 39
- events, setting local 23

## F

- factory defaults, restoring 33
- fan speed monitoring 38
- firmware, updating 48
- forwarding alerts from ISMP 19

## G

- gateway to forward ISMP alerts 19
- global login settings (Web interface) 16
- GMT offset in time setting 14
- graphical console, redirecting 45

## H

- host server startup sequence, changing 5

## I

- initialization-string guidelines for modem 26
- ISMP alert forwarding 19
- ISMP vital product data, viewing 42

## L

- loader watchdog (server timeout) 12
- local events, setting 23
- logging in to a Remote Supervisor Adapter 3
- logging off Web interface 34
- login profiles
  - creating 15
  - setting access rights 15
- login settings, global (Web interface) 16

## M

- machine level vital product data, viewing 40
- modem settings, configuring (global login) 25
- modem, initialization-string guidelines for 26
- modifying ASM configuration 33

## N

- navigation links available 5
- network interfaces
  - configuring Ethernet connection 26
- network protocols
  - configuring DNS 31
  - configuring SMTP 31
  - configuring SNMP 29
- NMI reset delay for server restart 13

notices and statements 2

## O

operating system (OS) watchdog (server timeout) 12

## P

pager codes

critical alerts 21

system alerts 22

warning alerts 22

POST events, viewing 39

POST watchdog (server timeout) 11

POST/BIOS vital product data, viewing 41

power and restart for server

activity 43

remote control 44

power off delay for server shutdown 13

profiles, login

creating 15

setting access rights 15

protocols

DNS 31

SMTP 31

SNMP 29

PXE Boot Agent 5

## R

remote alert attempts, setting 20

remote alert recipients, configuring 17

remote alerts, setting

critical 21

system 22

warning 22

remote boot 46

remote control

accessing server graphical console 45

overview 45

remote control keys 46

remote control of server power 44

remote disk 46

remote servers, monitoring

fan speed 38

temperature thresholds 36

voltage thresholds 37

Remote Supervisor Adapter

action descriptions 5

features 1

logging in to (Web interface) 3

restarting ASM 34

restoring ASM configuration 33

restoring ASM defaults 33

## S

server event log

severity levels 39

viewing 39

server power and restart

activity 43

remote control 44

server text console, viewing 45

server timeouts, setting

in Web interface 11

setting

local events 23

system information 10

settings, configuring

global login (Web interface) 16

SMTP, configuring 31

SNMP, configuring 29

startup sequence, changing 5

system alerts 22

system health, monitoring

fan speed 38

summary page 35

temperature thresholds 36

voltage thresholds 37

system information, setting

in Web interface 10

## T

temperature monitoring 36

timeouts, setting server 11

trademarks 54

## U

updating firmware 48

users logged in 5

## V

vital product data (VPD), viewing 40

voltages monitoring 37

## W

warning alerts 22

watchdog (server timeout)

loader 12

operating system (OS) 12

POST 11

Web browser requirements 2





Part Number: 88P9243

Printed in U.S.A.

(1P) P/N: 88P9243

