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 85.

Third Edition (November 2003)

Contents

Chapter 1. Introduction

This document explains how to use the functions of the IBM® Remote Supervisor Adapter II when you install it in an IBM @server 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

Your Remote Supervisor Adapter II documentation might be updated occasionally to include information about new features, a translated version of the documentation might be available in your language, or technical updates might be available to provide additional information that is not included in your adapter documentation. These updates are available from the IBM Web site. Complete the following steps to check for updated documentation and technical updates:

1. Go to http://www.ibm.com/pc/support/.
2. In the **Learn** section, click **Online publications**.
3. On the “Online publications” page, in the **Brand** field, select **Servers**.
4. In the **Family** field, select **Rack/Storage Enclosures**.
5. Click **Display documents**.

Important: Moving the Remote Supervisor Adapter II from one server type (for example, an IBM @server xSeries® 235) to another server type (for example, an IBM @server xSeries 345) is not supported.

Remote Supervisor Adapter II features

The Remote Supervisor Adapter II has the following standard features:

- Access to critical server settings
- Access to server vital product data (VPD)
- Advanced Predictive Failure Analysis® (PFA) support
- Alphanumeric or numeric pager alerts
- Automatic notification and alerts
- Automated Server Restart (ASR)
- Continuous health monitoring and control
- Domain Name System (DNS) server support
- Dynamic Host Configuration Protocol (DHCP) support
- E-mail alerts
- Enhanced user authority Levels
- Event logs that are time stamped, saved on the Remote Supervisor Adapter II, and can be attached to e-mail alerts
- Independent power, which enables around-the-clock access to the server even when the server power is off
- LAN and Advanced System Management (ASM) interconnect remote access
- Operating-system-failure screen capture
- Remote access through Ethernet and ASM interconnect peer-to-peer network

- Remote disk enabling the attachment of a diskette drive, CD-ROM drive, or disk image to a server
- Remote firmware update and access to critical server settings
- Remote power control
- Seamless remote accelerated graphics
- Secure Web server user interface
- Server console redirection
- Simple Network Management Protocol (SNMP) support
- Remote firmware update
- User authentication using a secure connection to a Lightweight Directory Access Protocol (LDAP) server

Web browser and operating system requirements

The Remote Supervisor Adapter II Web interface requires the Java™ Plug-in 1.4 or later and one of the following Web browsers:

- If the client system is running a Microsoft® Windows® operating system:
  - Microsoft Internet Explorer version 5.5 or later with the latest Service Pack
  - Netscape Navigator version 7.0 or later
- If the client system is running a Linux operating system:
  - Mozilla version 1.3 or later (Remote Control features are not supported.)

The following server operating systems have USB support, which is required for the Remote Control feature:

- Microsoft Windows Server 2003
- Microsoft Windows 2000 with Service Pack 4 or later
- Red Hat Linux version 7.3
- SuSE Linux version 8.0

Note: 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 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

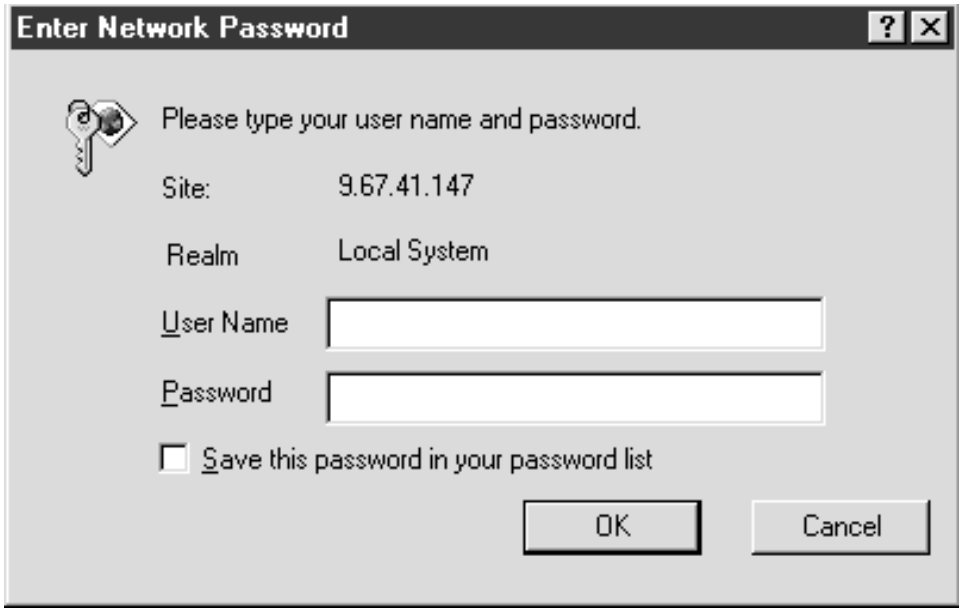
Complete the following steps to access the Remote Supervisor Adapter II through the Remote Supervisor Adapter II Web interface:

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 DHCP-assigned IP address or the static IP address from the server BIOS or from your network administrator.

   The Enter Network Password window opens.

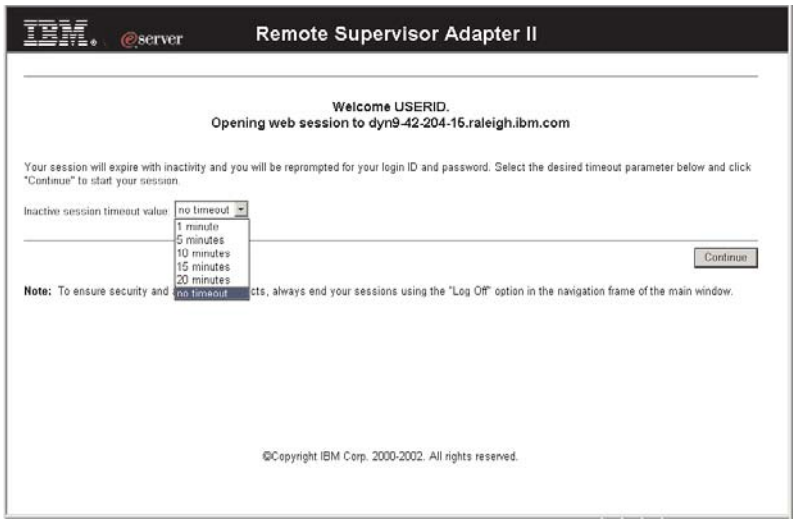
   Note: The values in the following window are examples. Your settings will be different.



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 PASSW0RD (with a zero, not an O). This user has read/write access. Change this default password during your initial

configuration for enhanced security.

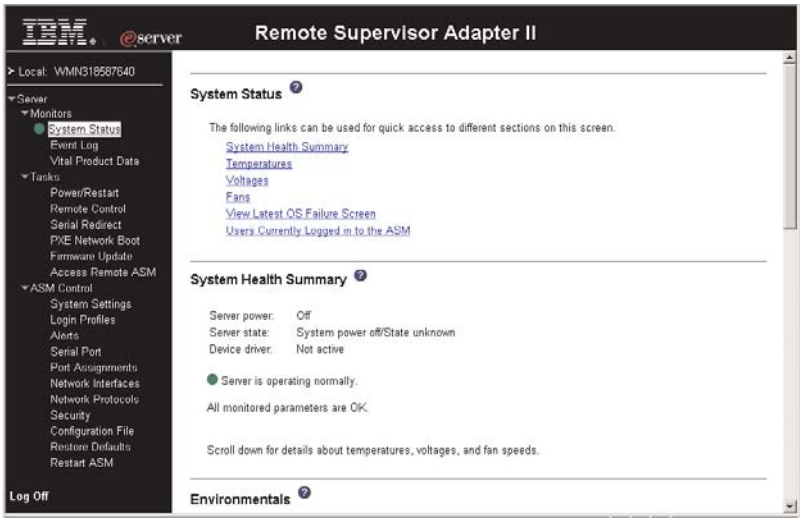


3. Select a timeout value from the drop-down list in the field provided. If your browser is inactive for that number of minutes, the Remote Supervisor Adapter II logs you off the Remote Supervisor Adapter II Web interface.

   Note: Depending on how your system administrator has configured the global login settings, the timeout value might be a fixed value.

4. Click **Continue** to start the session.

   The browser opens the System Status page, which gives you a quick view of the server status and the server health summary.



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 the 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.
Serial Redirect	Configure serial-to-serial redirection or serial-to-Telnet redirection.	From the Serial Redirect page, you can use the serial redirection quick setup to simplify the configuration of serial-to-serial redirection or serial-to-Telnet redirection.
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. **Note:** *Service processors* 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 and global login settings	You can define 12 login profiles that enable access to the Remote Supervisor Adapter II. You can also define global login settings that apply to all login profiles, including enabling Lightweight Directory Access Protocol (LDAP) server authentication.
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 ports and modem settings	From the Serial Port page, you can configure the serial ports and modem settings used by the Remote Supervisor Adapter II. You can also configure the serial redirect and command-line interface (CLI) settings.
Port assignments	Change the port numbers of the Remote Supervisor Adapter II protocols.	From the Port Assignments page, you can change the port numbers of Remote Supervisor Adapter II protocols (for example, HTTP, HTTPS, Telnet, and SNMP).
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. You can also configure the point-to-point protocol (PPP) access through the Remote Supervisor Adapter II serial port.
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. You can also configure LDAP parameters.

Table 1. Remote Supervisor Adapter II actions (continued)

Link	Action	Description
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 certificates that are used. You can also enable or disable whether an SSL connection is used to connect to an LDAP server.
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.
Restore Defaults	Restore the Remote Supervisor Adapter II defaults	**Attention:** When you click **Restore Defaults**, 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 the 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 (Microsoft Windows or Linux)

    Attention:

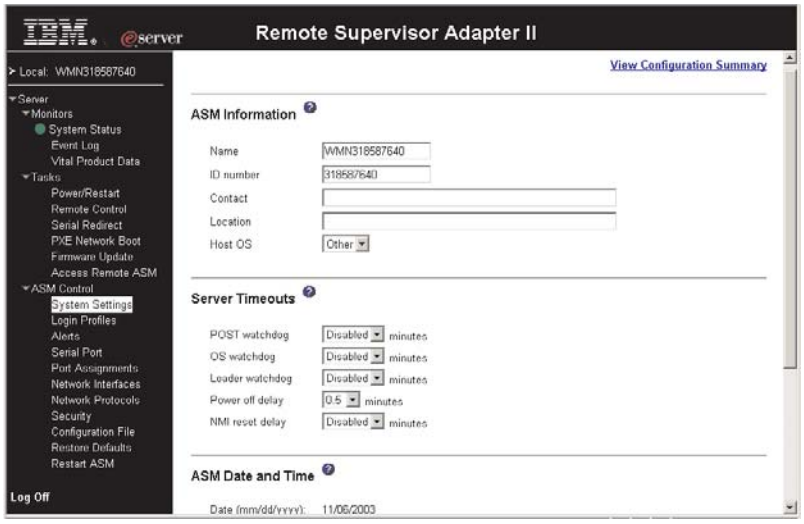
    - For the Remote Supervisor Adapter II to function properly, the specified operating system must match the operating system of the server in which the Remote Supervisor Adapter II is installed.
    - Set this selection to Linux before attempting to install Linux device drivers.
  - Set server timeouts
  - 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 ports of the Remote Supervisor Adapter II
  - Configure advanced modem settings
  - Set up serial redirection
- From the Port Assignments page, you can change the port numbers of Remote Supervisor Adapter II services.
- From the Network Interfaces page, you can:
  - Set up the Ethernet connection for the Remote Supervisor Adapter II
  - Set up a PPP over serial port connection
- From the Network Protocols page, you can:
  - Configure SNMP setup
  - Configure DNS setup
  - Configure SMTP setup
  - Configure LDAP setup
- From the Security page, you can install and configure the Secure Sockets Layer (SSL) settings.
- 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 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:

   1. 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).
   2. 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 35.

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.
6. 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.
7. In the **HOST O/S** menu, click the type of operating system that is running on the server.

   Attention:

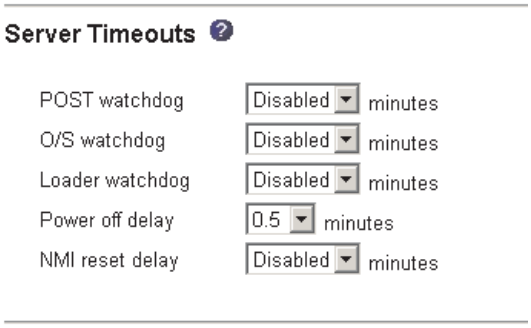
   - The operating system that you specify must match the operating system in the server for the Remote Supervisor Adapter II to function properly.
   - Set this selection to **Linux** before attempting to install Linux device drivers. The default setting is **Windows**.
8. Scroll to the bottom of the page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

Setting server timeouts

Complete the following steps to set your server timeout values:

1. 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 interface,” on page 3.
2. 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.



   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
3. 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 means that the server is turned off and then immediately turned on.

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:

1. 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*.
2. 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:

1. 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.
2. 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, Windows Server 2003, 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**.

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

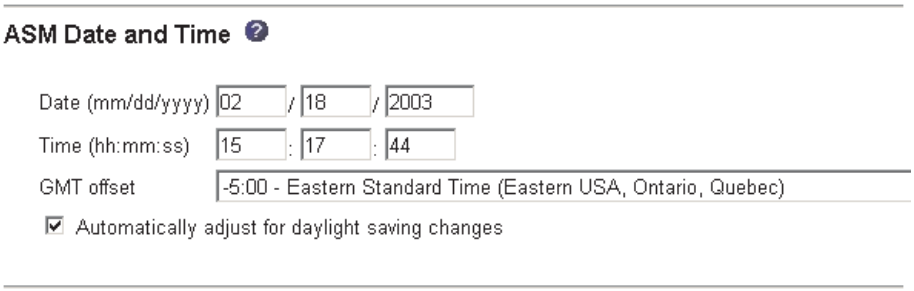
Setting the date and time

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 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.



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 ~`.

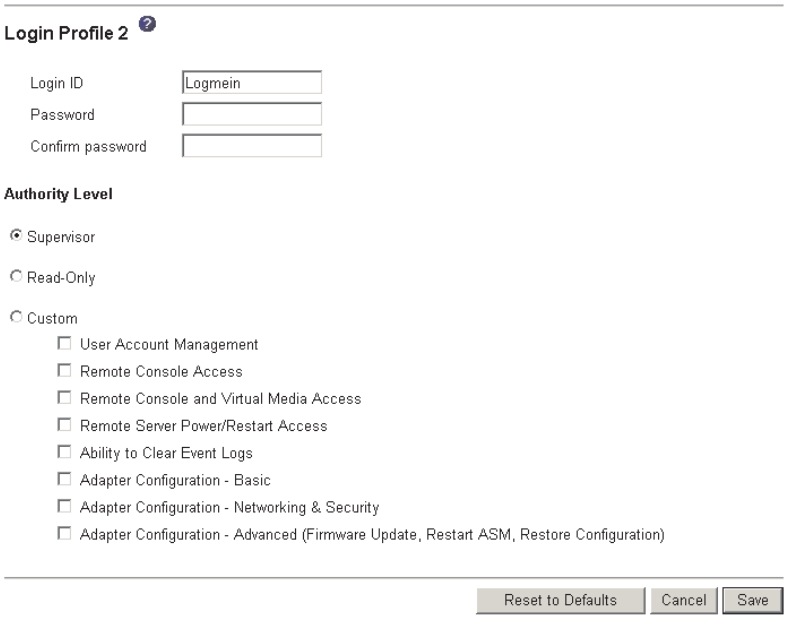
Complete the following steps to configure a login profile:

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 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 `PASSW0RD` (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 is displayed.



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 **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.

6. In the **Confirm Password** field, type the password again.
7. In the **Authority level** section, select one of the following options to set the access rights for this login ID:

   Supervisor
   The user has no restrictions.

   Read Only
   The user has read-only access only, and cannot perform actions such as file transfers, power and restart actions, or remote control functions.

   Custom
   If you select the Custom option, you must select one or more of the following custom authority levels:

   - **User Account Management:** A user can add, modify, or delete users and change the global login settings in the Login Profiles page.
   - **Remote Console Access:** A user can access the remote console.
   - **Remote Console and Virtual Media Access:** A user can access both the remote console and the virtual media feature.
   - **Remote Server Power/Restart Access:** A user can access the power on and restart functions for the remote server. These functions are available in the Power/Restart page.
   - **Ability to Clear Event Logs:** A user can clear the event logs. Everyone can look at the event logs, but this particular permission is required to clear the logs.
   - **Adapter Configuration - Basic:** A user can modify configuration parameters in the System Settings and Alerts pages.
   - **Adapter Configuration - Networking & Security:** A user can modify configuration parameters in the Security, Network Protocols, Network Interface, Port Assignments, and Serial Port pages.
   - **Adapter Configuration (Advanced):** A user has no restrictions when configuring the adapter. In addition, the user is said to have administrative access to the Remote Supervisor Adapter II, meaning that the user can also perform the following advanced functions: firmware updates, PXE network boot, restore adapter factory defaults, modify and restore adapter configuration from a configuration file, and restart and reset the adapter.

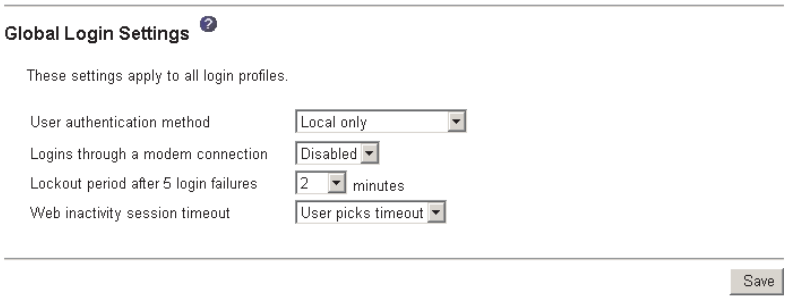
8. Click **Save** to save your login ID settings.

Configuring 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 interface,” on page 3.
2. In the navigation pane, click **Login Profiles**.

3. Scroll down to the Global Login Settings section. A page similar to the one in the following illustration is displayed.



4. In the **User authentication method** field, specify how users attempting to log in are authenticated. Select one of the following authentication methods.
   - **Local only.** Users are authenticated by searching a table local to the Remote Supervisor Adapter II. If there is no match on the user ID and password, access is denied. Users who are successfully authenticated are assigned the authority level configured in “Creating a login profile” on page 14.
   - **LDAP only**. The Remote Supervisor Adapter II attempts to authenticate the user using the LDAP server. Local user tables on the Remote Supervisor Adapter II are never searched with this authentication method.
   - **Local first, then LDAP**. Local authentication is attempted first. If local authentication fails, LDAP authentication is attempted.
   - **LDAP first, then Local**. LDAP authentication is attempted first. If LDAP authentication fails, local authentication is attempted.
5. In the **Logins through a modem connection** field, select **Enabled** to allow PPP users to dial in to the Remote Supervisor Adapter II using a modem connection.
6. In the **Lockout period after 5 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.
7. In the **Web inactivity session timeout** field, specify how long, in minutes, the Remote Supervisor Adapter II will wait before disconnecting an inactive Web session. Select **no timeout** to disable this feature. Select **User picks timeout** if the user will select the timeout period during the login process.
8. Click **Save**.

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 39.
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.

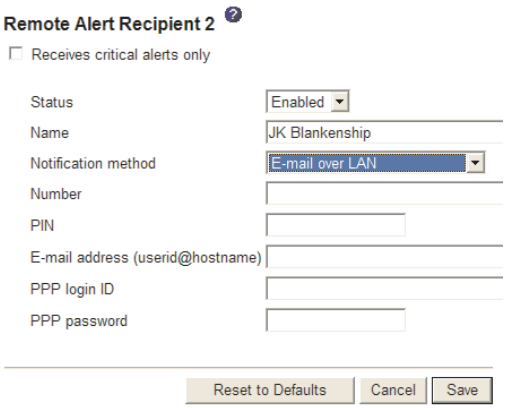
Configuring remote alert recipients

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 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.



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 type 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

   Note: To configure a remote alert recipient for IBM Director over Modem or IBM Director over LAN, the remote alert recipient must be a server on which IBM Director Server is 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 41.

11. In the **PPP login ID** field, specify the login ID or user ID needed to log in to your Internet Service Provider (ISP).

    Note: The **PPP login ID** field is required for E-mail over PPP and SNMP over PPP notification methods. For remote access on a Windows operating system, this is usually the user ID of the account that is set up.

    For example, to log in to the IBM Global Network®, the PPP login ID is in the following format: secureip.*y.z* where *y* is your account name, and *z* is your user ID.

12. In the **PPP password** field, type the password used to log in to the ISP.

    This field is required only for E-mail over PPP and SNMP over PPP notification methods.

13. Click **Save** to save your remote alert recipient profile. Repeat step 2 on page 18 through step 10 on page 19 for each remote alert recipient profile.
14. 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.

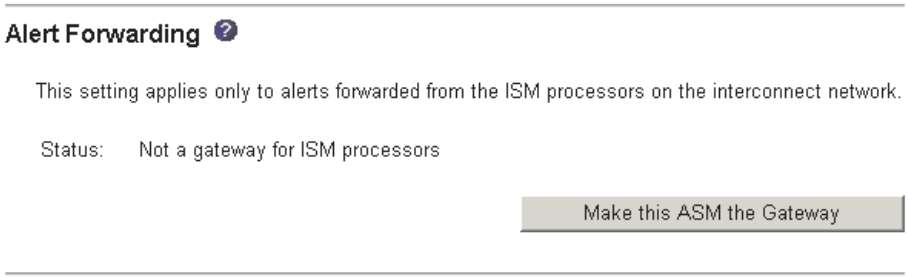
Notes:

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 interface,” on page 3.
2. In the navigation pane, click **Alerts** and scroll down to the **Alert Forwarding** section.



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

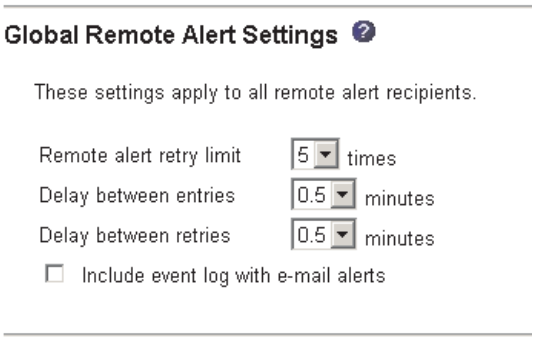
Setting remote alert attempts

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 interface,” on page 3.

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



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:

   1. 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.
   2. 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 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.
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.

Table 3. Warning remote alerts (continued)

Alphanumeric pager code	Alphanumeric recovery code	Event	Action
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:

1. The **Select all system alerts** check box is not available on all servers.
2. Hard disk drive Predictive Failure Analysis (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 **Server Timeouts** 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 **Server Timeouts** 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 **Generate Test Alert** 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 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.
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.

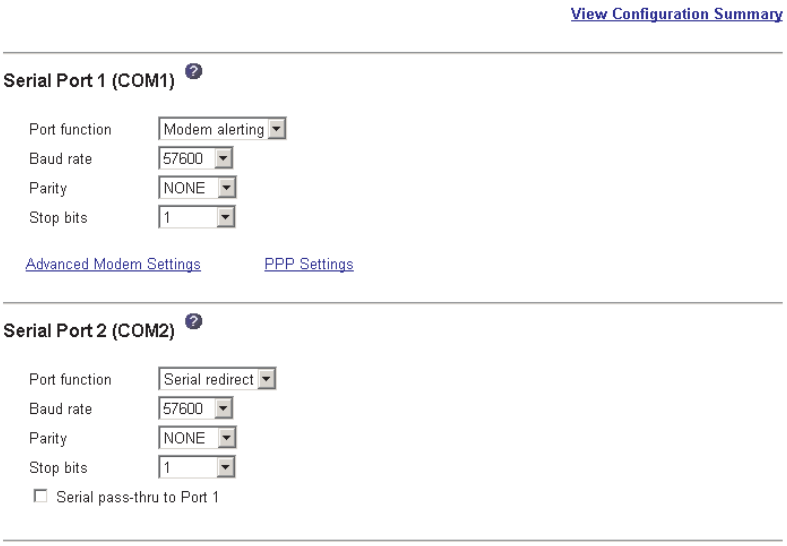
4. Scroll to the bottom of the page and click **Save**.

Configuring the serial connectors

Note: If your Remote Supervisor Adapter II came with an ASM breakout cable with a single serial connector, you can configure only serial port 1.

Complete the following steps to configure the serial connector:

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 interface,” on page 3.
2. In the navigation pane, click **Serial Port**. A page similar to the one in the following illustration is displayed.

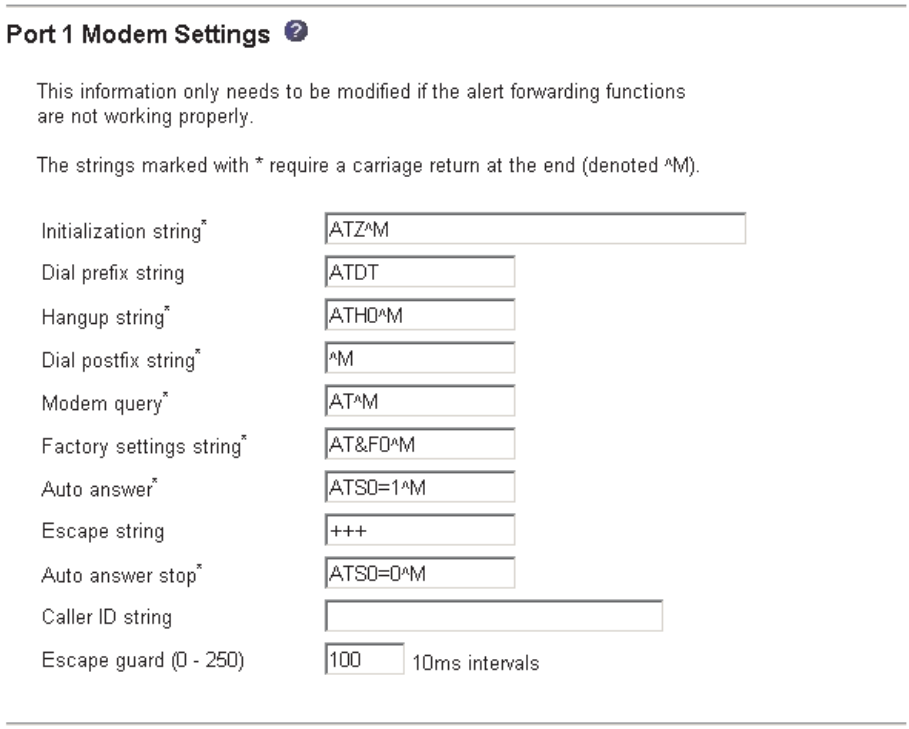


3. In the **Port function** field, select the function for which this serial port will be used. If the Remote Supervisor Adapter II supports point-to-point protocol (PPP) over a serial port, select **PPP** as the port function to enable the PPP interface for that port. Any other selection disables the PPP interface. Select **None**, if available, to disables the port. If you select **PPP**, click **PPP Settings** to configure the settings. For more information, see “Configuring PPP access over a serial connection” on page 38.
4. 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.
5. In the **Parity** field, select the error detection to be used in your serial connection.
6. 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.
7. Click **Save**.

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



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.
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 +++.

Table 6. Port 1 settings (continued)

Field	What you type
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.

9. 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:

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

Configuring the dual serial connectors for serial redirection

If your Remote Supervisor Adapter II came with an ASM breakout cable with dual serial connectors, use the information in this section to configure the serial connectors for serial redirection.

You can use the ASM breakout cable with dual serial connectors to connect the server serial port (using a null modem cable) to a client workstation using a terminal-emulation program such as Hilgraeve HyperTerminal or to a hardware terminal server (also using a null modem cable). The Remote Supervisor Adapter II acts as a pass-through device. Using this single serial connection to a terminal server or client workstation, a system administrator can access the serial features of both the operating system and the Remote Supervisor Adapter II. The Remote Supervisor Adapter II command-line interface (CLI) provides text-based power control and server reset ability.

To use the ASM breakout cable with dual serial connectors for a single serial connection to a terminal server, make sure that:

- Your server basic input/output system (BIOS) code supports the single serial connection. This BIOS serial support is needed to provide power-on self-test (POST), setup, and end-to-end remote access.
- You update the Remote Supervisor Adapter II firmware. For information about obtaining Remote Supervisor Adapter II firmware and software, see the *Installation Guide*.
- Your operating system has serial support for text management in the operating system. The following operating systems have serial support:
  - Microsoft Windows Server 2003 Enterprise Edition with emergency management services for serial console support
  - Linux operating systems with Agetty serial console support

Serial-to-serial redirection

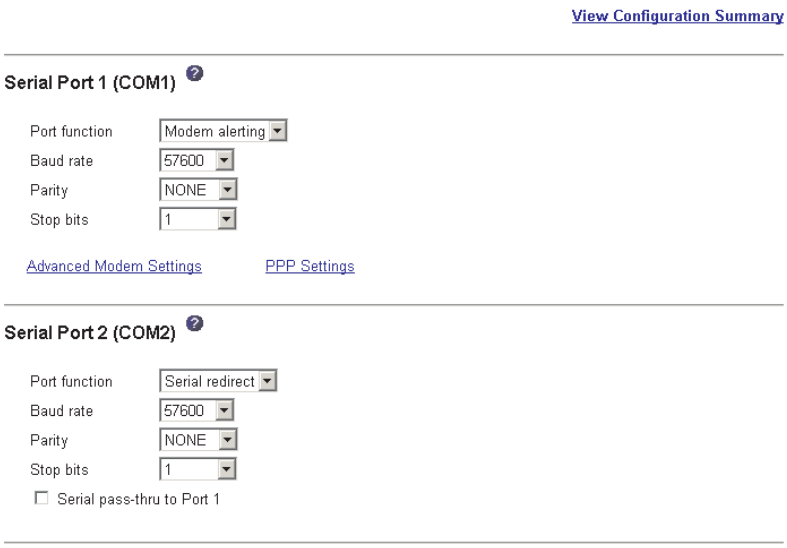
Serial-to-serial redirection enables the Remote Supervisor Adapter II to pass data between COM1 and COM2. This mode is useful when a single serial connection is required to a client computer or a hardware terminal server.

When serial authentication is enabled, the serial command-line interface session is authenticated using the local logon profiles or using an LDAP server.

For serial redirection quick setup information, see “Serial redirection quick setup” on page 78.

Complete the following steps to set up the software configuration for serial-to-serial redirection configuration:

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 interface,” on page 3.
2. In the navigation pane, click **Serial Port**. A page similar to the one in the following illustration is displayed.



3. In the **Serial Port 1** section, set the following values for the fields:
   a. In the **Port function** field, select **Serial redirect**.

Note: The serial ports are enabled independently for serial redirection. For serial-to-serial redirection, both ports must be set to serial redirect. The available options for COM1 are modem alerting, PPP, and serial redirect. COM2 supports only serial redirection, if it is enabled.

b. Configure the **Baud rate**, **Parity**, and **Stop bits** fields to match the serial port settings on the server.

Notes:

1. Serial redirection does not support hardware-based flow control. Disable the terminal flow control.
2. To prevent buffer overrun and character loss, configure both serial ports with the same baud rate. The Remote Supervisor Adapter II provides a 512-character buffer on both incoming and outgoing serial streams.

4. In the **Serial Port 2** section, set the following values for the fields:
   a. In the **Port function** field, select **Serial redirect**.
   b. Configure the **Baud rate**, **Parity**, and **Stop bits** fields to match the serial port settings on the server.

   Note: Serial redirection does not support hardware-based flow control. Disable the terminal flow control.
5. Click the **Serial pass-thru to Port 1** check box. This check box forces the link between COM1 and COM2. Both ports must be active and in serial redirection mode to enable this function. If the function is not enabled, the command-line interface must be invoked and the console command must be used to link the appropriate ports together.

Serial-to-Telnet redirection

Serial-to-Telnet redirection enables a system administrator to use the Remote Supervisor Adapter II as a serial terminal server. Either one or both serial ports can be accessed from a Telnet connection when serial redirection is enabled.

For serial redirection quick setup information, see “Serial redirection quick setup” on page 78.

The Remote Supervisor Adapter II uses the custom command-line interface enter key sequence to return from a serial redirection session. The command-line interface enter key sequence defaults to the Microsoft Windows Server 2003 emergency management services compatible key sequence: Press Esc (.

Notes:

1. The Remote Supervisor Adapter II allows two open Telnet sessions. The Telnet sessions can independently access the serial ports allowing multiple users to have a concurrent view of a redirected serial port.
2. One serial port must be enabled for serial redirection to enable the **console** command.
3. Telnet does not make use of the command-line interface exit key sequence. The command-line interface **console** command must be used to select a COM port.
4. The Telnet session is authenticated using the local logon profiles or using an LDAP server.

Example session

```
telnet 192.168.70.125 (Press Enter.)
Connecting to 192.168.70.125...
username: USERID (Press Enter.)
```

```
password: ******** (Press Enter.)
SN# J1RAE32S000> console 1 (Press Enter.)
unsupported console
SN# J1RAE32S000> console 2 (Press Enter.)
```

Note: All traffic from COM2 is now routed to the Telnet session. All traffic from the Telnet session is routed to COM2.

```
ESC (
```

Note: In the default mode (EMS compatible), ESC (will return to the command-line interface.

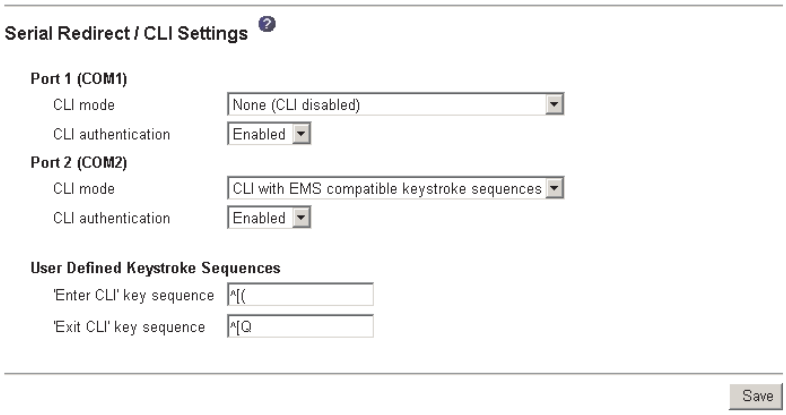
```
SN# J1RAE32S000> exit (Press Enter.)
```

Configuring the command-line interface settings

The Remote Supervisor Adapter II provides a basic set of commands for reset and power control. The command-line interface is available from either or both serial ports and from up to two simultaneous Telnet sessions. The Remote Supervisor Adapter II offers the following set of reset and power commands: console, exit, help, power, reset, and resetsp.

Complete the following steps to use the command-line interface:

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 interface,” on page 3.
2. In the navigation pane, click **Serial Port**.
3. Scroll to the **Serial Redirect Settings / CLI Settings** section.



4. Use the following information to select the values for the fields.

CLI mode

The command-line interface mode options allow the administrator to configure whether the command-line interface is available from a serial port and whether a custom key sequence must be used to enter and exit. The default mode allows the Remote Supervisor Adapter II to function in Microsoft Windows Server 2003-compatible environments.

Select from the following values:

- **None (CLI disabled)**

  The Remote Supervisor Adapter II does not allow access to the command-line interface from this serial port.
- **CLI with EMS compatibility keystroke sequences**

The Remote Supervisor Adapter II accepts three key sequences when in Emergency Management Services-compatible mode. The sequences are defined by the Microsoft Windows Server 2003 Emergency Management Services specification. The key sequences that are supported are in the following table.

Table 7. Supported Emergency Management Services key sequences

Task	Key sequence
Enter the Remote Supervisor Adapter II command-line interface	Press Esc (The Remote Supervisor Adapter II sends Esc * as an acknowledgement to the command.
Exit the command-line interface	Press Esc Q
Reset the server	Press Esc R Esc r Esc R No authentication is required to reset the server in this mode.

- **CLI with user defined keystroke sequences**

  The Remote Supervisor Adapter II accepts the enter and exit sequences defined in the “Enter CLI” key sequence and “Exit CLI” key sequence. The fields are defined in the following sections. The Remote Supervisor Adapter II does not provide a server reset key sequence in this mode.

CLI authentication

The command-line interface can be automatically invoked when a user types the “Enter CLI” key sequence. This mode is provided for environments where the serial port is secured outside Remote Supervisor Adapter II. Telnet sessions always require the user to authenticate.

Select from the following values:

- **Enabled**

  A username/password prompt is presented. Authentication is required to get access to the command-line interface commands.

- **Disabled**

  No username/password is presented when the enter command-line interface key sequence is pressed. The serial port has full access to all available commands.

User Defined Keystroke Sequences

The enter key sequence specifies the key sequence that the Remote Supervisor Adapter II will require to begin a command-line interface session. The exit key sequence specifies the key sequence that is required to exit from the command-line interface.

When you select **CLI with user defined keystroke sequences** for the serial port, the serial port (COM1 and COM2) sessions use the custom command-line interface enter and exit key sequences.

The Telnet sessions always use the custom command-line interface enter key sequence to return to the Remote Supervisor Adapter II command-line interface.

The sequences can be up to 19 characters. Control characters are specified on the Web interface using the Caret key (^).

The default sequences will be equivalent to the EMS key sequences. When **CLI with user defined keystroke sequence** is selected, the EMS reset key sequence is not available and the Remote Supervisor Adapter II will not issue the EMS acknowledgement when the enter key sequence is accepted.

5. At the bottom of the page, click **Save**.
6. To begin using the new settings, in the left navigation pane, click **Restart ASM**.

To set up the hardware connections, see the *Installation Guide*.

Using the command-line interface

The following commands are available from both the Telnet command-line interface and the serial command-line-interface.

console

The **console** command connects the current session to a serial port. The serial port must be active for serial redirection or the command will return unsupported. Press Esc (or the user-defined key sequence to return to the command-line interface.

Examples:

The following command attempts to attach the current session to COM1:

```
console 1
```

The following command attempts to attach the current session to COM2:

```
console 2
```

exit The **exit** command exits from the command-line interface session. The session is closed forcing re-authentication.

help The **help** command reports the available commands.

power The **power** command reports or sets the power state of the connected server. The power control is available only for servers connected to the Remote Supervisor Adapter II internal management connector. The available options are:

-on (To turn on power) For example, power -on.

-off (To turn off power)

-state (To return the state of the system power, either on or off)

reset The **reset** command forces the system to reset.

resetsp

The **resetsp** command issues the reset command to the Remote Supervisor Adapter II firmware. Five seconds later, the Remote Supervisor Adapter II firmware will close the connection and restart.

Configuring port assignments

Complete the following steps to change the port numbers of Remote Supervisor Adapter II services.

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

2. In the navigation pane, click **Port Assignments**. A page similar to the one in the following illustration is displayed.

3. Use the following information to assign values for the fields:

   HTTP This is the port number for the HTTP server of the Remote Supervisor Adapter II. The default port number is 80. Other valid values are in the range 1 through 65535. If you change this port number, you will need to add this port number preceded by a colon at the end of the Web address. For example, if the HTTP port is changed to 8500, you would type `http://hostname:8500/` to open the Remote Supervisor Adapter II Web interface. Note that you must type the prefix `http://` before the IP address and port number.

   HTTPS
   This is the port number used for Web interface HTTPS (SSL) traffic. The default value is 443. Other valid values are in the range 1 through 65535.

   Telnet This is the port number for the Telnet server of the Remote Supervisor Adapter II. The default value is 23. Other valid values are in the range 1 through 65535.

   SNMP Agent
   This is the port number for the SNMP agent running on the Remote Supervisor Adapter II. The default value is 161. Other valid values are in the range 1 through 65535.

   SNMP Traps
   This is the port number used for SNMP traps. The default value is 162. Other valid values are in the range 1 through 65535.

   The following port numbers are reserved and can be used only for the corresponding services.

Table 8. Reserved port numbers

Port number	Services used for
2000	Video redirect
4444	Remote disk
4445	Remote disk on card
6090	IBM Director access
247	SLP
7070 through 7074	Partition management

4. Click **Save**.

Configuring network interfaces

On the Network Interfaces page, you can set access to the Remote Supervisor Adapter II by:

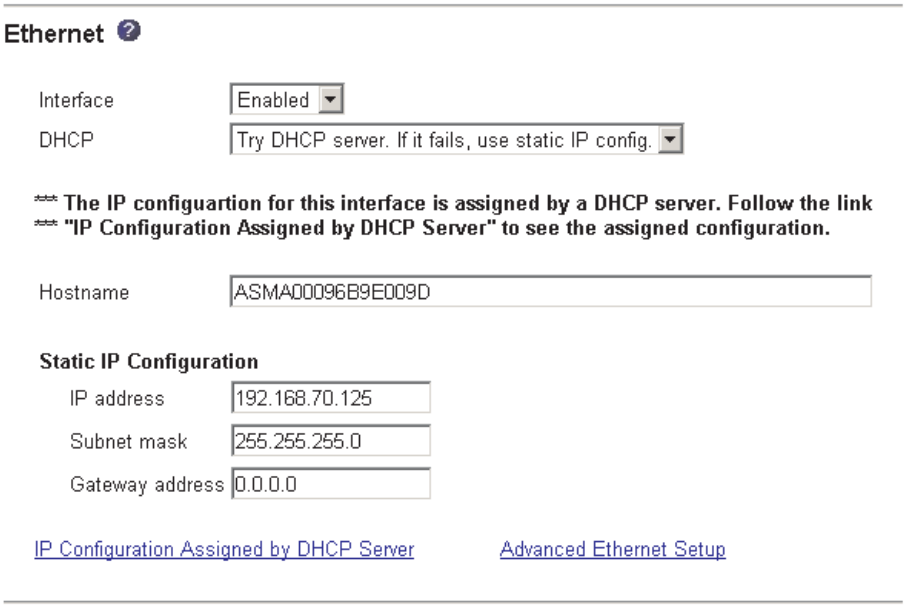
- Configuring an Ethernet connection to a Remote Supervisor Adapter II
- Configuring point-to-point protocol access over a serial connector

Configuring an Ethernet connection to the Remote Supervisor Adapter II

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 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.



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 37.

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

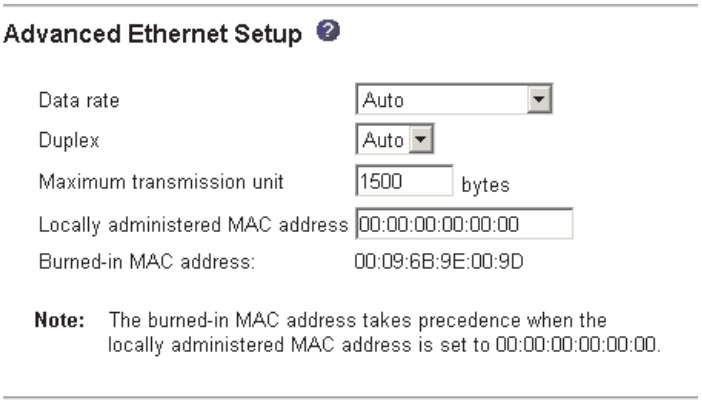
5. Type the IP host name of the Remote Supervisor Adapter II in the **Hostname** field.

   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.



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

Table 9. Advanced Ethernet setup

Field	Function
Data rate	Use the **Data Rate** 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[1], that corresponds to the capability of your network. To automatically detect the data-transfer rate, select **Auto**, which is the default value.
Duplex	Use the **Duplex** field to specify the type of communication channel used in your network. To set the duplex mode, select one of the following choices: **Full** enables data to be carried in both directions at once. **Half** enables data to be carried in either one direction or the other, but not both at the same time. To automatically detect the duplex type, select **Auto**, which is the default value.
Maximum transmission unit	Use the **Maximum transmission unit** 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.
Burned-in MAC address	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.
Locally administered MAC address	Enter a physical address for this Remote Supervisor Adapter II in the **Locally administered MAC address** 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 FFFFFFFFFFFF. 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.
[1]Mb equals approximately 1 000 000 bits.	

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 PPP access over a serial connection

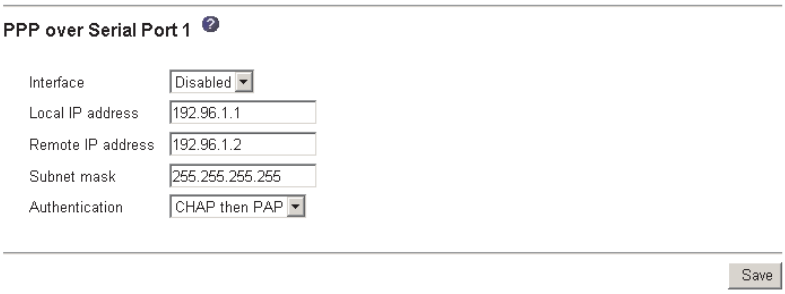
Use the point-to-point protocol (PPP) access method if you do not have Ethernet access. You can use PPP through your serial port to enable access to the Remote Supervisor Adapter II through a Telnet session or a Web browser.

Note: If you enable the PPP interface, the Remote Supervisor Adapter II cannot use the serial port for serial remote access.

Complete the following steps to configure PPP access over a serial port:

1. Log in to the Remote Supervisor Adapter where you want to configure PPP access over a serial port. For more information, see Chapter 2, “Opening and using the Web interface,” on page 3..
2. In the navigation pane, click **Network Interfaces**. Scroll down to the PPP over Serial Port 1 section.

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



3. In the **Interface** field, select **Enabled**.
4. In the **Local IP address** field, type the local IP address for the PPP interface on this Remote Supervisor Adapter II. The field defaults to 192.96.1.1. The IP address must contain:
   - Four integers from 0 through 255 separated by periods
   - No spaces
5. In the **Remote IP address** field, type the remote IP address that this Remote Supervisor Adapter II will assign to a remote user. The field defaults to 192.96.1.2. The remote IP address must contain:
   - Four integers from 0 through 255 separated by periods
   - No spaces
6. In the **Subnet mask** field, type the subnet mask for the Remote Supervisor Adapter II to use. The default is 255.255.255.255. The subnet mask must contain:
   - Four integers from 0 through 255 separated by periods

- No spaces

7. In the **Authentication** field, specify the type of authentication protocol that will be negotiated when a PPP connection is attempted.
   - The **PAP Only** setting uses a two-way handshake procedure to validate the identity of the originator of the connection. The weak privileged access protection (PAP) authentication protocol is necessary if a plain text password must be available to simulate a login at a remote host.
   - The **CHAP Only** setting uses a three-way handshake procedure to validate the identity of the originator of a connection upon connection at any time later. The challenge handshake authentication protocol (CHAP) is stronger than the PAP protocol and protects against playback and trial-and-error attacks.
   - The **CHAP then PAP** setting tries to authenticate using CHAP first. If the originator of the connection does not support CHAP, then PAP is tried as a secondary authentication protocol. The **CHAP then PAP** setting is the default.
8. Click **Save**.
9. 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 Lightweight Directory Access Protocol (LDAP)

Configuring SNMP

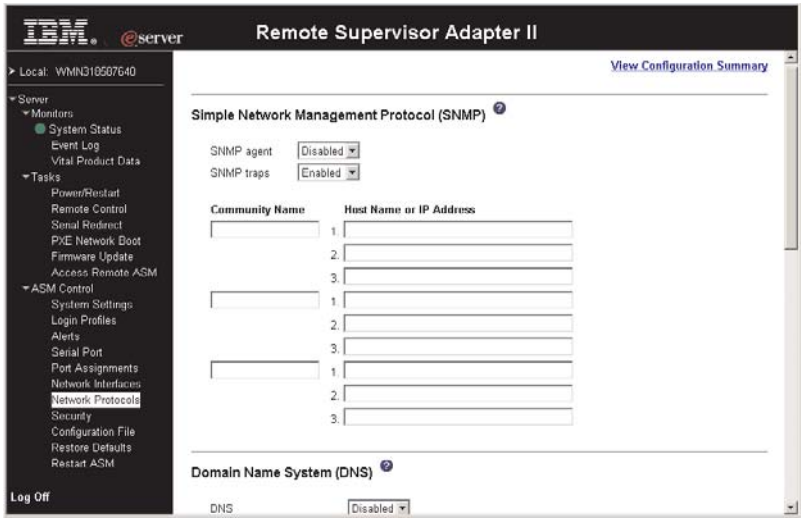
You can query the SNMP agent to collect the sysgroup information and to send configured SNMP alerts to the configured host names or IP addresses.

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 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.



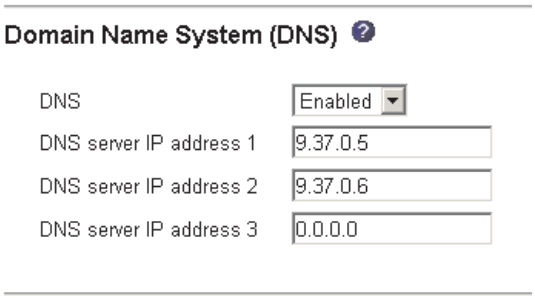
5. Select **Enabled** in the **SNMP agent** and **SNMP traps** fields to forward alerts to SNMP communities on your network. To enable the SNMP agent, the following criteria must be met:
   - System contacts must be specified on the System Settings page. For information about the System Settings page 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.



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 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**.

Configuring LDAP

Using a Lightweight Directory Access Protocol (LDAP) server, a Remote Supervisor Adapter II can authenticate a user by querying or searching an LDAP directory on an LDAP server, instead of going through its local user database. Then, all Remote Supervisor Adapter IIs can remotely authenticate any user access through a central LDAP server. This requires LDAP client support on the Remote Supervisor Adapter II. You can also assign authority levels based on information found on the LDAP server.

You can also use LDAP to assign users and Remote Supervisor Adapter IIs to groups, and perform group authentication, in addition to the normal user (password check) authentication. For example, a Remote Supervisor Adapter II can be

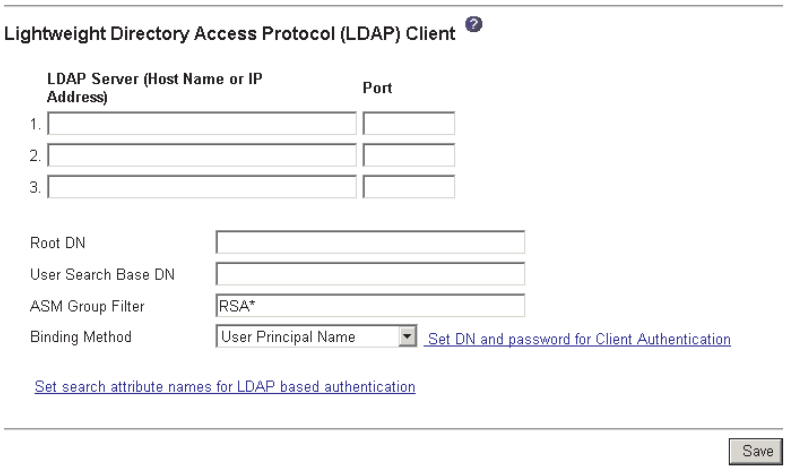
associated with one or more groups, and a user would only pass group authentication if he belongs to at least one group associated with the Remote Supervisor Adapter II.

Note: LDAP-based authentication for PPP sessions is not supported.

Setting up a client to use the LDAP server

Complete the following steps to set up a client to use the LDAP server:

1. Log in to the Remote Supervisor Adapter II where you want to set up the client. For more information, see Chapter 2, “Opening and using the Web interface,” on page 3.
2. In the navigation pane, click **Network protocols**. Scroll down to the Lightweight Directory Access Protocol (LDAP) Client section. A page similar to the one in the following illustration is displayed.



3. Configure the LDAP client using the following information:

   LDAP Server

   The Remote Supervisor Adapter II contains a Version 2.0 LDAP client that you can configure to provide authentication through a centrally located LDAP server. You can configure up to three LDAP servers. The port number for each server is optional. If left blank, the default value of 389 is used for non-secured LDAP connections. For secured connections, the default is 636. You must configure at least one LDAP server.

   Root DN

   The distinguished name for the root entry of the directory tree on the LDAP server. An example might look like dn=companyABC,dn=com.

   User Search Base DN

   As part of the user authentication process, it is necessary to search the LDAP server for one or more attributes associated with a particular user. Any search request must specify the base distinguished name for the actual search. The **User Search Base DN** field specifies the base distinguished name that is used to search the user directory. An example might look like cn=Users,dn=companyABC,dn=com. If this field is left blank, the root distinguished name is used as the search base.

   User searches are part of the authentication process. They are carried out to retrieve information about the user such as login permissions, callback number, and group memberships. For Version 2.0 LDAP

clients, be sure to configure this parameter; otherwise, a search using the root distinguished name might not succeed (as seen on Microsoft Windows Server 2003 Active Directory servers).

ASM Group Filter

This parameter is used for group authentication. It specifies the set of groups to which this particular Remote Supervisor Adapter II belongs. If left blank, group authentication is disabled. Otherwise, group authentication is performed against this filter. The filter specified can be a specific group name (for example, RSAWest), a wildcard with a prefix (for example, RSA*), or a wildcard (specified as *). If a specific name is used, this Remote Supervisor Adapter II belongs only to this group. If a prefix filter is used (for example, RSA*), this Remote Supervisor Adapter II belongs to any group whose first three letters are RSA. If a wildcard filter (*) is used, then this Remote Supervisor Adapter II belongs to all groups. The default filter is RSA*.

Group authentication is performed after user authentication (where a user ID and password are verified). Group authentication refers to the process of verifying that a user is a member of at least one group associated with this Remote Supervisor Adapter II. For example, assume the group filter is set to RSA*. If the user belongs to two groups, for example, Engineering and RSAWest, group authentication passes because the user belongs to a group (RSAWest) that matches the filter RSA*. If the groups to which the user belong do not match the filter, group authentication fails and the user is not allowed to access the Remote Supervisor Adapter II. Note that if the group filter is *, then group authentication will automatically succeed because any group to which the user belongs will match this wildcard.

Binding Method

For initial binds to the LDAP server during user authentication, choose from the following options:

Anonymous authentication. A bind attempt is made without a client distinguished name or password. If the bind is successful, a search will be requested to find an entry on the LDAP server for the user attempting to log in. If an entry is found, a second attempt to bind will be attempted, this time with the distinguished name and password of the user. If this succeeds, the user has passed the user authentication phase. Group authentication is then attempted if it is enabled.

Client authentication. A bind attempt is made with the client distinguished name and password specified by this configuration parameter. If the bind is successful, the user authentication phase proceeds as in Anonymous authentication.

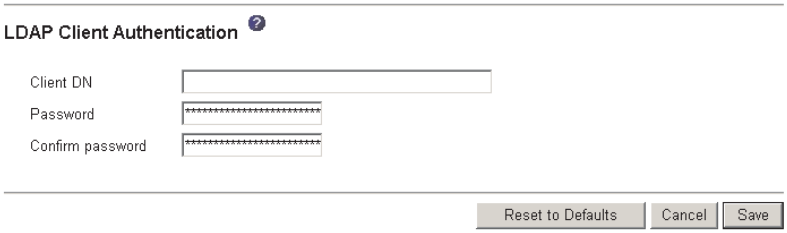
User Principal Name. A bind attempt is made directly with the credentials used during the login process. If this succeeds, the user has passed the user authentication phase. The user principal name usually refers to a fully qualified name, such as johndoe@abc.com. However, johndoe would also be acceptable.

Strict User Principal Name. This is similar to the user principal name, except that a fully qualified name must be entered by the user. That is, johndoe@abc.com would be acceptable, but not johndoe. The name entered by the user will be parsed for the @ symbol.

Configuring the LDAP client authentication

Complete the following steps to configure the LDAP client authentication:

1. In the navigation pane, click **Network protocols**.
2. Scroll down to the Lightweight Directory Access Protocol (LDAP) Client section and click **Set DN and password for Client Authentication**. A page similar to the one in the following illustration is displayed.



3. The initial bind to the LDAP server during user authentication can be performed with anonymous authentication, client-based authentication, or user principle name. To use client-based authentication, in the **Client DN** field, type a client distinguished name. Type a password in the **Password** field or leave it blank.

Configuring the LDAP search attributes

Complete the following steps to configure the LDAP search attributes:

1. In the navigation pane, click **Network protocols**.
2. Scroll down to the Lightweight Directory Access Protocol (LDAP) Client section and click **Set search attribute names for LDAP based authentication**. A page similar to the one in the following illustration is displayed.

3. To configure the search attributes, use the following information.

UID Search Attribute

When the binding method selected is Anonymous authentication or Client authentication, the initial bind to the LDAP server is followed by a search request directed at retrieving specific information about the user, including the distinguished name, login permissions, and group ownerships of the user. To retrieve this information, the search request must specify the attribute name used to represent user IDs on that server. Specifically, this name is used as a search filter against the login ID entered by the user. This attribute name is configured here. If this field is left blank, a default of UID is used during user authentication. For example, on Active Directory servers, the attribute name used for user IDs is often sAMAccoutName.

When the binding method selected is User principal name or Strict user principal name, the **UID Search Attribute** field defaults automatically to userPrincipalName during user authentication if the user ID entered has the form userid@somedomain.

Group Search Attribute

When the Group Filter name is configured, it is necessary to retrieve from the LDAP server the list of groups to which a particular user belongs. This is required to perform group authentication. To retrieve this list, the search filter sent to the server must specify the attribute name associated with groups. This field specifies this attribute name.

If this field is left blank, the attribute name in the filter will default to memberOf.

Login Permission Attribute

When a user is successfully authenticated using an LDAP server, the login permissions for this user must be retrieved. To retrieve these permissions, the search filter sent to the server must specify the attribute name associated with login permissions. This field specifies this attribute name.

If this field is left blank, the user is assigned a default of read-only permissions, assuming user and group authentication passes.When successfully retrieved, the attribute value returned by the LDAP server is interpreted according to the following information:

- It must be a bit string entered as 12 consecutive zeros or ones, with each bit representing a particular set of functions. For example: 010000000000 or 000011001000. The bits are numbered according to their position. The leftmost bit is bit position 0, and the rightmost bit is bit position 11. A value of 1 at a particular position enables that particular function. A value of 0 disables that function. There are 12 available bits, which are described in the following list:
  - Deny Always (bit position 0): If set, a user will always fail authentication. This function can be used to block a particular user or users associated with a particular group.
  - Supervisor Access (bit position 1): If set, a user is given administrator privileges. The user has read and write access to every function. When this bit is set, the other bits below do not have to be set individually.
  - Read Only Access (bit position 2): If set, a user has read-only access and cannot perform any maintenance procedures (for example, restart, remote actions, and firmware updates), and nothing can be modified (using the save, clear, or restore functions). Note that read-only and all other bits are mutually exclusive, with read-only having the lowest precedence. That is, if any other bit is set, this bit will be ignored.
  - Networking & Security (bit position 3): If set, a user can modify the configuration in the Security, Network Protocols, Network Interface, Port Assignments, and Serial Port pages.
  - User Account Management (bit position 4): If set, a user can add, modify, and delete users and change the Global Login Settings in the Login Profiles page.
  - Remote Console Access (bit position 5): If set, a user can access the remote server console.
  - Remote Console and Virtual Media Access (bit position 6): If set, a user can access the remote server console and the virtual media functions for the remote server.
  - Remote Server Power/Restart Access (bit position 7): If set, a user can access the power on and restart functions for the remote server. These functions are available in the Power/Restart page.

  - Basic Adapter Configuration (bit position 8): If set, a user can modify configuration parameters in the System Settings and Alerts pages.
  - Ability to Clear Event Logs (bit position 9): If set, a user can clear the event logs. Everyone can look at the event logs, but this particular permission is required to clear the logs.
  - Advanced Adapter Configuration (bit position 10): If set, a user has no restrictions when configuring the adapter. In addition, the user is said to have administrative access to the Remote Supervisor Adapter II, meaning that the user can also perform the following advanced functions: firmware upgrades, PXE network boot, restore adapter factory defaults, modify and restore adapter configuration from a configuration file, and restart and reset the adapter.
  - Reserved (bit position 11): Reserved for future use.
- If none of the bits are set, the default will be set to read-only for the user.
- Priority is given to login permissions retrieved directly from the user record. If the user does not have the login permission attribute in its record, an attempt will be made to retrieve the permissions from the groups to which the user belongs. This is done as part of the group authentication phase. The user will be assigned the inclusive OR of all the bits for all of the groups. The Browser Only bit will be set only if all the other bits are zero. If the Deny Always bit is set for any of the groups, the user will be refused access. The Deny Always bit always has precedence over every other bit.

Secure Web server and secure LDAP

Secure Sockets Layer (SSL) is a security protocol that provides communication privacy. SSL enables client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

You can configure the Remote Supervisor Adapter II to use SSL support for two types of connections: secure Web server (HTTPS) and secure LDAP connection (LDAPS). The Remote Supervisor Adapter II takes on the role of SSL client or SSL server depending on the type of connection. The following table shows that the Remote Supervisor Adapter II acts as an SSL server for secure Web server connections. The Remote Supervisor Adapter II acts as an SSL client for secure LDAP connections.

Table 10. Remote Supervisor Adapter II SSL connection support

Connection type	SSL client	SSL server
Secure Web server (HTTPS)	Web browser of the user (For example: Microsoft Internet Explorer)	A Remote Supervisor Adapter II Web server
Secure LDAP connection (LDAPS)	Remote Supervisor Adapter II LDAP client	An LDAP server

You can view or change the Secure Sockets Layer (SSL) settings from the Security page. You can enable or disable SSL and manage the certificates required for SSL.

Configuring security

Use the general procedure in this section to configure security for the Remote Supervisor Adapter II Web server and to configure security for the connection

between the Remote Supervisor Adapter II and an LDAP server. If you are not familiar with the use of SSL certificates, read the information in “SSL certificate overview” on page 48.

The content of the Security Web page is context-sensitive. The selections available on the page change when the SSL installation key is imported, when certificates or certificate signing requests are generated, when certificates are imported or removed, and when SSL is enabled or disabled for the client or the server.

Use the following general tasks list to configure the security for the Remote Supervisor Adapter II:

1. Install the SSL installation key. See “Installing the SSL key.” This step is performed only once when you install a new Remote Supervisor Adapter II in a server.
2. Configure the Secure Web server:
   a. Disable the SSL server. Use the SSL Server Configuration for Web Server section on the Security page.
   b. Generate or import a certificate. Use the SSL Server Certificate Management section on the Security page. (See “SSL server certificate management” on page 49.)
   c. Enable the SSL server. Use the SSL Server Configuration for Web Server section on the Security page. (See “Enabling SSL for the secure Web server” on page 54.)
3. Configure SSL security for LDAP connections:
   a. Disable the SSL client. Use the SSL Client Configuration for LDAP Client section on the Security page.
   b. Generate or import a certificate. Use the SSL Client Certificate Management section on the Security page. (See “SSL client certificate management” on page 54.)
   c. Import one or more trusted certificates. Use the SSL Client Trusted Certificate Management section on the Security page. (See “SSL client trusted certificate management” on page 55.)
   d. Enable the SSL client. Use the SSL Client Configuration for LDAP Client section on the Security page. (See “Enabling SSL for the LDAP client” on page 56.)
4. Restart the Remote Supervisor Adapter II for SSL server configuration changes to take effect. For more information, see “Restarting ASM” on page 60.

   Note: Changes to the SSL client configuration take effect immediately and do not require a restart of the Remote Supervisor Adapter II.

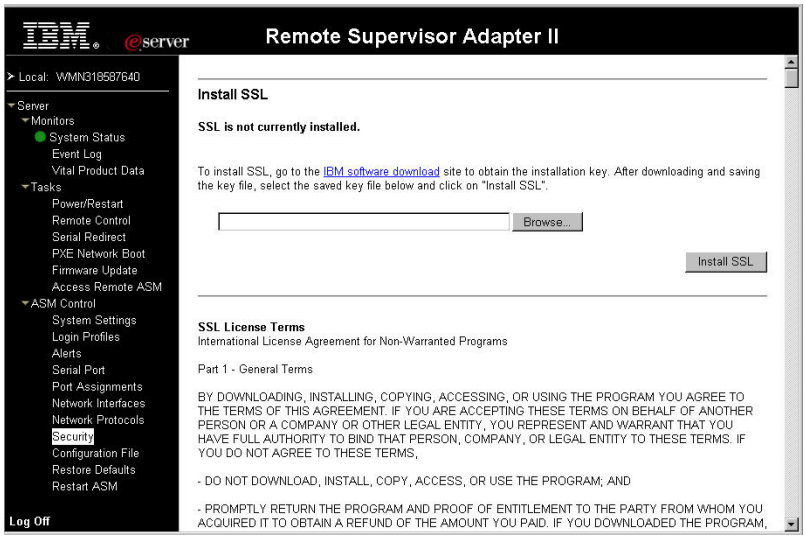
Installing the SSL key

The first time you select **Security** from the navigation pane, you are directed to an IBM Web page to verify that you meet United States export regulations for use of cryptographic software and to download the SSL installation key. After you install the key, you can configure and enable SSL.

Complete the following steps to install the SSL key:

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 interface,” on page 3.

2. In the navigation pane, click **Security**. If this is the first time you are selecting Security, a page similar to the one in the following illustration opens.



3. Download the SSL installation key according to the instructions on the Install SSL page. Click **Install SSL**.
4. On the Install SSL page, click **configure and enable**; then, complete the configuration using the information in the following sections.

SSL certificate overview

You can use SSL with either a self-signed certificate or with a certificate signed by a third-party certificate authority. Using a self-signed certificate is the simplest method for using SSL, but it does create a small security risk. The risk arises because the SSL client has no way of validating the identity of the SSL server for the first connection attempted between the client and server. It is possible that a third party could impersonate the server and intercept data flowing between the Remote Supervisor Adapter II and the Web browser. If at the time of the initial connection between the browser and the Remote Supervisor Adapter II, the self-signed certificate is imported into the certificate store of the browser, all future communications will be secure for that browser (assuming the initial connection was not compromised by an attack).

For more complete security, you can use a certificate signed by a certificate authority. To obtain a signed certificate, use the SSL Certificate Management page to generate a certificate signing request. You must then send the certificate signing request to a certificate authority and make arrangements to procure a certificate. When the certificate is received, it is then imported into the Remote Supervisor Adapter II using the **Import a Signed Certificate** link, and you can enable SSL.

The function of the certificate authority is to verify the identity of the Remote Supervisor Adapter II. A certificate contains digital signatures for the certificate authority and the Remote Supervisor Adapter II. If a well-known certificate authority issues the certificate or if the certificate of the certificate authority has already been imported into the Web browser, the browser will be able to validate the certificate and positively identify the Remote Supervisor Adapter II Web server.

The Remote Supervisor Adapter II requires a certificate for the secure Web server and one for the secure LDAP client. Also, the secure LDAP client requires one or more trusted certificates. The trusted certificate is used by the secure LDAP client

to positively identify the LDAP server. The trusted certificate is the certificate of the certificate authority that signed the certificate of the LDAP server. If the LDAP server uses self-signed certificates, the trusted certificate can be the certificate of the LDAP server itself. Additional trusted certificates must be imported if more than one LDAP server is used in your configuration.

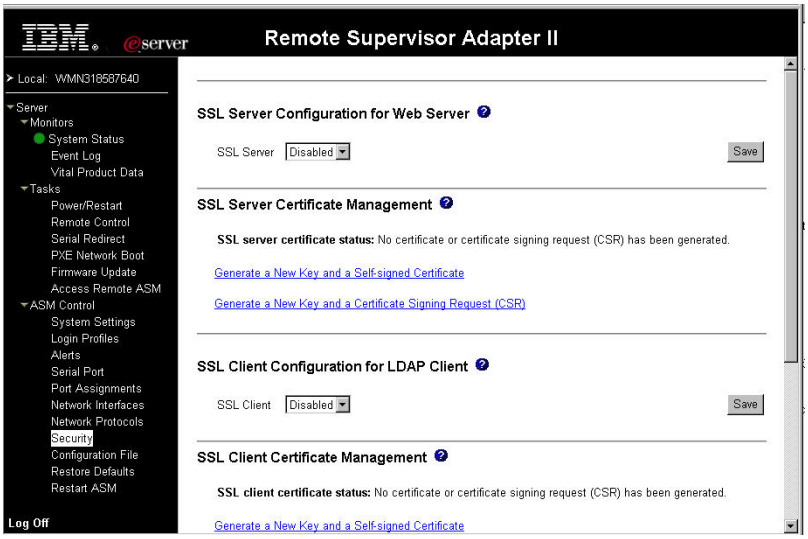
SSL server certificate management

The SSL server requires that a valid certificate and corresponding private encryption key is installed before SSL is enabled. There are two methods available for generating the private key and required certificate: using a self-signed certificate and using a certificate signed by a certificate authority. If you want to use a self-signed certificate for the SSL server, see “Generating a self-signed certificate.” If you want to use a certificate authority signed certificate for the SSL server, see “Generating a certificate signing request” on page 50.

Generating a self-signed certificate

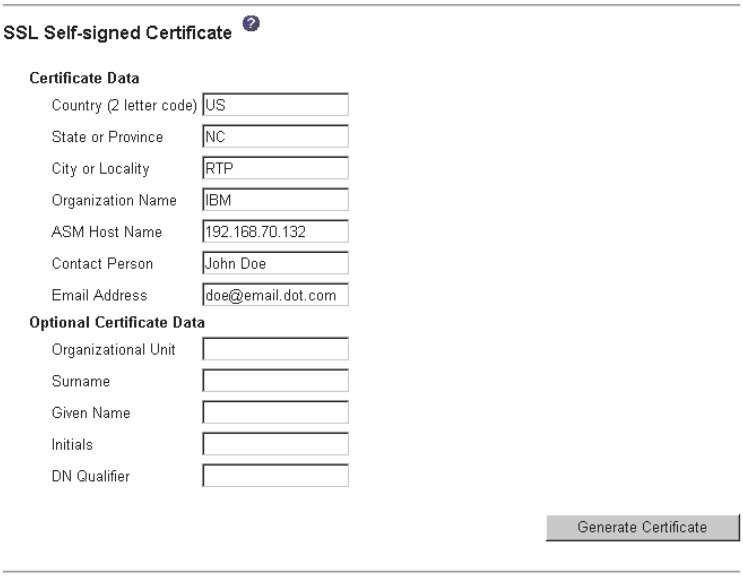
Complete the following steps to generate a new private encryption key and self-signed certificate:

1. In the navigation plane, click **Security**. A page similar to the one in the following illustration is displayed.



2. In the SSL Server Configuration for Web Server section, make sure that the SSL server is disabled. If it is not disabled, select **Disabled** in the **SSL Server** field and then click **Save**.
3. In the SSL Server Certificate Management section, select **Generate a New Key and a Self-signed Certificate**. A page similar to the one in the following

illustration is displayed.



4. Type the information in the required fields and any optional fields that apply to your configuration. For a description of the fields, see “Required certificate data” on page 51. After you finish typing the information, click **Generate Certificate**. Your new encryption keys and certificate are generated. This process might take several minutes.

   A page similar to the one in the following illustration is displayed and you can see that a self-signed certificate is installed.

Generating a certificate signing request

Complete the following steps to generate a new private encryption key and certificate signing request:

1. In the navigation pane, click **Security**.
2. In the SSL Server Configuration for Web Server section, make sure that the SSL server is disabled. If it is not disabled, select **Disabled** in the **SSL Server** field and then click **Save**.
3. In the SSL Server Certificate Management section, select **Generate a New Key and a Certificate Signing Request**. A page similar to the one in the

following illustration is displayed.

4. Type the information in the required fields and any optional fields that apply to your configuration. The fields are the same as the self-signed certificate with some additions.

   Read the information in the following sections for a description of each of the common fields.

   Required certificate data

   The following user-input fields are required for generating a self-signed certificate or a certificate signing request.

   Country

   Use this field to indicate the country where the Remote Supervisor Adapter II physically resides. This field must contain the 2-character country code.

   State or Province

   Use this field to indicate the state or province where the Remote Supervisor Adapter II physically resides. This field can contain a maximum of 30 characters.

   City or Locality

   Use this field to indicate the city or locality where the Remote Supervisor Adapter II physically resides. This field can contain a maximum of 50 characters.

   Organization Name

   Use this field to indicate the company or organization that owns the Remote Supervisor Adapter II. When this is used to generate a certificate signing request, the issuing certificate authority can verify that the organization requesting the certificate is legally entitled to claim ownership of the given company or organization name. This field can contain a maximum of 60 characters.

   ASM Host Name

   Use this field to indicate the Remote Supervisor Adapter II host name that currently appears in the browser Web address bar.

Make sure that the value you typed in the **ASM host name** field exactly matches the host name as it is known by the Web browser. The browser compares the host name in the resolved Web address to the name that appears in the certificate. To prevent certificate warnings from the browser, the value used in this field must match the host name used by the browser to connect to the Remote Supervisor Adapter II. For example, if the Web address bar in the browser currently is http://mm11.xyz.com/private/main.ssi, the value used for the **ASM Host Name** field must be mm11.xyz.com. If the Web address is http://mm11/private/main.ssi, the value used must be mm11. If the Web address is http://192.168.70.2/private/main.ssi, the value used will be 192.168.70.2.

This certificate attribute is generally referred to as the common name.

This field can contain a maximum of 60 characters.

Contact Person

Use this field to indicate the name of a contact person responsible for the Remote Supervisor Adapter II. This field can contain a maximum of 60 characters.

Email Address

Use this field to indicate the e-mail address of a contact person responsible for the Remote Supervisor Adapter II. This field can contain a maximum of 60 characters.

Optional certificate data

The following user-input fields are optional for generating a self-signed certificate or a certificate signing request.

Organizational Unit

Use this field to indicate the unit within the company or organization that owns the Remote Supervisor Adapter II. This field can contain a maximum of 60 characters.

Surname

Use this field for additional information, such as the surname of a person responsible for the Remote Supervisor Adapter II. This field can contain a maximum of 60 characters

Given Name

Use this field for additional information, such as the given name of a person responsible for the Remote Supervisor Adapter II. This field can contain a maximum of 60 characters.

Initials

Use this field for additional information, such as the initials of a person responsible for the Remote Supervisor Adapter II. This field can contain a maximum of 20 characters.

DN Qualifier

Use this field for additional information, such as a distinguished name qualifier for the Remote Supervisor Adapter II. This field can contain a maximum of 60 characters.

Certificate signing request attributes

The following fields are optional unless they are required by your selected certificate authority.

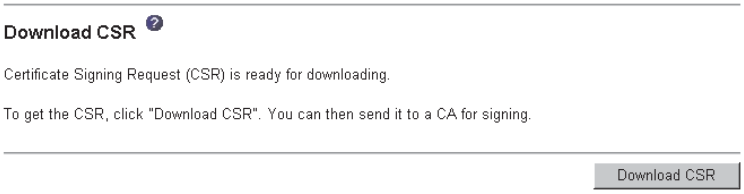
Challenge Password

Use this field to assign a password to the certificate signing request. This field can contain a maximum of 30 characters.

Unstructured Name

Use this field for additional information, such as an unstructured name assigned to the Remote Supervisor Adapter II. This field can contain a maximum of 60 characters.

5. After completing the information, click **Generate CSR**. The new encryption keys and certificate are generated. This process might take several minutes. A page similar to the one in the following illustration is displayed when the process is completed.



6. Click **Download CSR** and then click **Save** to save the file to your workstation. The file produced when you create a certificate signing request is in DER format. If your certificate authority expects the data in some other format, such as PEM, the file can be converted using a third-party tool such as OpenSSL (http://www.openssl.org). If the certificate authority asks you to copy the contents of the certificate signing request file into a Web browser window, PEM format is usually expected.

   The command for converting a certificate signing request from DER to PEM format using OpenSSL is similar to the following:

   ```
   openssl req -in csr.der -inform DER -out csr.pem -outform PEM
   ```

7. Send the certificate signing request to your certificate authority. When the certificate authority returns your signed certificate it might be necessary to convert the certificate to DER format. (If you received the certificate as text in an e-mail or a Web page, it is probably in PEM format.) You can change the format using a tool provided by your certificate authority or using a third-party tool such as OpenSSL (http://www.openssl.org). The command for converting a certificate from PEM to DER format is similar to the following:

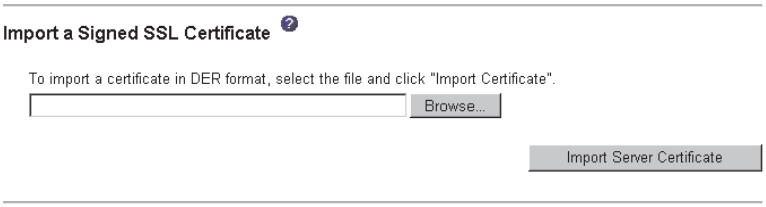
   ```
   openssl x509 -in cert.pem -inform PEM -out cert.der -outform DER
   ```

   Go to step 8 after the signed certificate is returned from the certificate authority.

8. In the navigation pane, click **Security**. Scroll to the SSL Server Certificate Management section, which looks similar to the page in the following

illustration.

9. Select **Import a Signed Certificate**. A page similar to the one in the following illustration is displayed.



10. Click **Browse**.
11. Click the certificate file that you want and then click **Open**. The file name (including the full path) is displayed in the field next to the **Browse** button.
12. Click **Import Server Certificate** to begin the process. A progress indicator is displayed as the file is transferred to storage on the Remote Supervisor Adapter II. Remain on this page until the transfer is completed.

Enabling SSL for the secure Web server

Note: To enable SSL, you must have a valid SSL certificate installed.

Complete the following steps to enable the secure Web server:

1. In the navigation pane, click **Security**. The page that is displayed looks similar to the one in the following illustration and shows that a valid SSL server certificate is installed. If the SSL server certificate status does not show that a valid SSL certificate is installed, go to “SSL server certificate management” on page 49.

2. Scroll to the SSL Server Configuration for Web Server section and select **Enabled** in the **SSL Client** field and then click **Save**. The value selected takes effect the next time the Remote Supervisor Adapter II is restarted.

SSL client certificate management

The SSL client requires that a valid certificate and corresponding private encryption key is installed before SSL is enabled. There are two methods available for

generating the private key and required certificate: using a self-signed certificate, or using a certificate signed by a certificate authority.

The procedure for generating the private encryption key and certificate for the SSL client is the same as the procedure for the SSL server, except that you use the SSL Client Certificate Management section of the Security Web page instead of the SSL Server Certificate Management section. If you want to use a self-signed certificate for the SSL client, see “Generating a self-signed certificate” on page 49. If you want to use a certificate authority signed certificate for the SSL client, see “Generating a certificate signing request” on page 50.

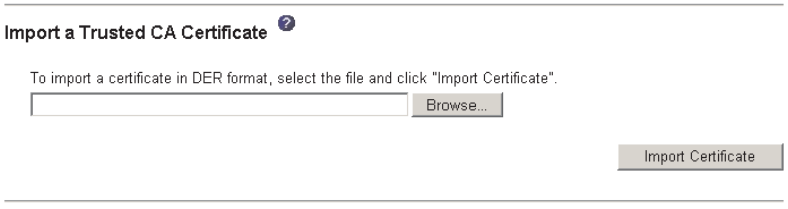
SSL client trusted certificate management

The secure SSL client (LDAP client) uses trusted certificates to positively identify the LDAP server. A trusted certificate can be the certificate of the certificate authority that signed the certificate of the LDAP server or it can be the actual certificate of the LDAP server. At least one certificate must be imported to the Remote Supervisor Adapter II before the SSL client is enabled. You can import up to three trusted certificates.

Complete the following steps to import a trusted certificate:

1. In the navigation pane, select **Security**.
2. In the SSL Client Configuration for LDAP Client section, make sure that the SSL client is disabled. If it is not disabled, select **Disabled** in the **SSL Client** field and then click **Save**.
3. Scroll to the SSL Client Trusted Certificate Management section. A page similar to the one in the following illustration is displayed.

4. Click **Import** next to one of the **Trusted CA Certificate 1** fields. A page similar to the one in the following illustration is displayed.



5. Click **Browse**.
6. Select the certificate file that you want and click **Open**. The file name (including the full path) is displayed in the box beside the **Browse** button.
7. To begin the import process, click **Import Certificate**. A progress indicator is displayed as the file is transferred to storage on the Remote Supervisor Adapter II. Remain on this page until the transfer is completed.

8. The SSL Client Trusted Certificate Management section of the Security page will now look similar to the one in the following illustration.

The **Remove** button is now available for the Trusted CA Certificate 1 option. If you want to remove a trusted certificate, click the corresponding **Remove** button.

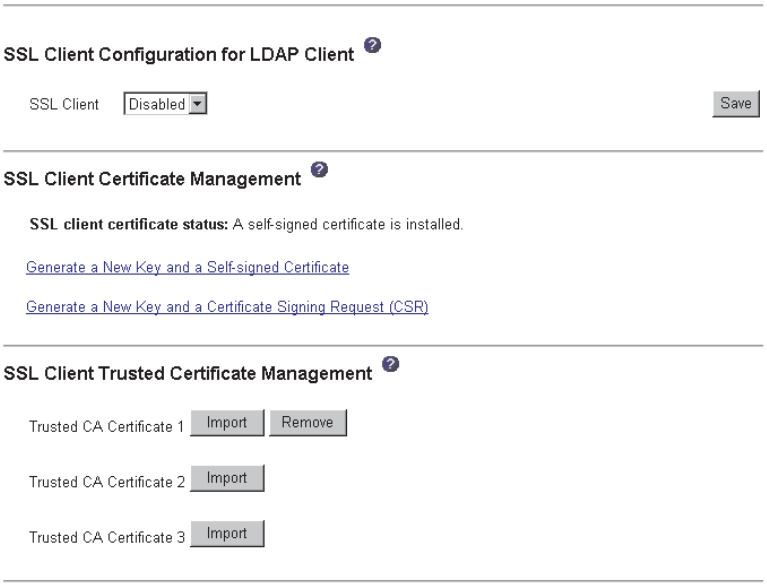
You can import other trusted certificates using the Trusted CA Certificate 2 and the Trusted CA Certificate 3 **Import** buttons.

Enabling SSL for the LDAP client

Use the SSL Client Configuration for LDAP Client section of the Security page to enable or disable SSL for the LDAP Client. To enable SSL, a valid SSL client certificate and at least one trusted certificate must first be installed.

Complete the following steps to enable SSL for the client:

1. In the navigation pane, click **Security**. A page similar to the one in the following illustration is displayed.



The Security page shows an installed SSL client certificate and Trusted CA Certificate 1.

2. On the SSL Client Configuration for LDAP Client page, select **Enabled** in the **SSL Client** field.
3. Click **Save**. The value selected takes effect immediately.

Configuring the secure shell server

Note: The secure shell server feature is not available on all servers.

The Secure Shell (SSH) feature provides secure access to the command-line interface and the serial (text console) redirect features of the Remote Supervisor Adapter II.

Secure shell users are authenticated by exchanging user ID and password. The password and user ID are sent after the encryption channel is established. The user ID and password pair can be one of the 12 locally stored user IDs and passwords or they can be stored on an LDAP server. Public key authentication is not supported.

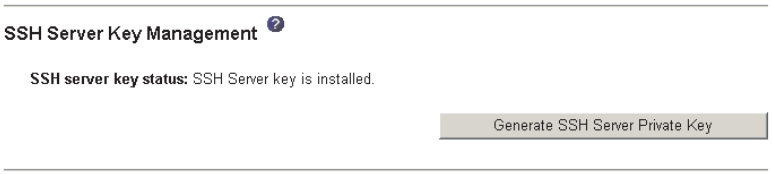
Generating a secure shell server key

A secure shell server key is used to authenticate the identity of the secure shell server to the client. Secure shell must be disabled before you create a new secure shell server private key. You must create a server key before enabling the secure shell server.

When you request a new server key, both a Rivest, Shamir, and Adelman key and a DSA key are created to allow access to the Remote Supervisor Adapter II from either a SSH version 1.5 or SSH version 2 client. For security, the secure shell server private key is not backed-up during a configuration save and restore operation.

Complete the following steps to create a new secure shell server key:

1. In the navigation pane, click **Security**.
2. Scroll to the Secure Shell (SSH) Server section and make sure that the secure shell server is disabled. If it is not disabled, select **Disabled** in the **SSH Server** field and then click **Save**.
3. Scroll to the SSH Server Key Management section. A page similar to the one in the following illustration is displayed.



4. Click **Generate SSH Server Private Key**. A progress window is displayed. Wait for the operation to be completed.

Enabling the secure shell server

From the Security page you can enable or disable the secure shell server. The selection that you make takes effect only after the Remote Supervisor Adapter II is restarted. The value displayed on the screen (Enabled or Disabled) is the last value selected and is the value used when the Remote Supervisor Adapter II is restarted.

Note: You can enable the secure shell server only if a valid secure shell server private key is installed.

Complete the following steps to enable the secure shell server:

1. In the navigation pane, click **Security**.
2. Scroll to the Secure Shell (SSH) Server section. A page similar to the one in the following illustration is displayed.

3. Click **Enabled** in the **SSH Server** field.
4. In the navigation pane, click **Restart ASM** to restart the Remote Supervisor Adapter II.

Using the secure shell server

If you are using the secure shell client that is included in Red Hat Linux version 7.3, to start a secure shell session to a Remote Supervisor Adapter II with network address 192.168.70.132, type a command similar to the following example:

```
ssh -x -l USERID 192.168.70.132
```

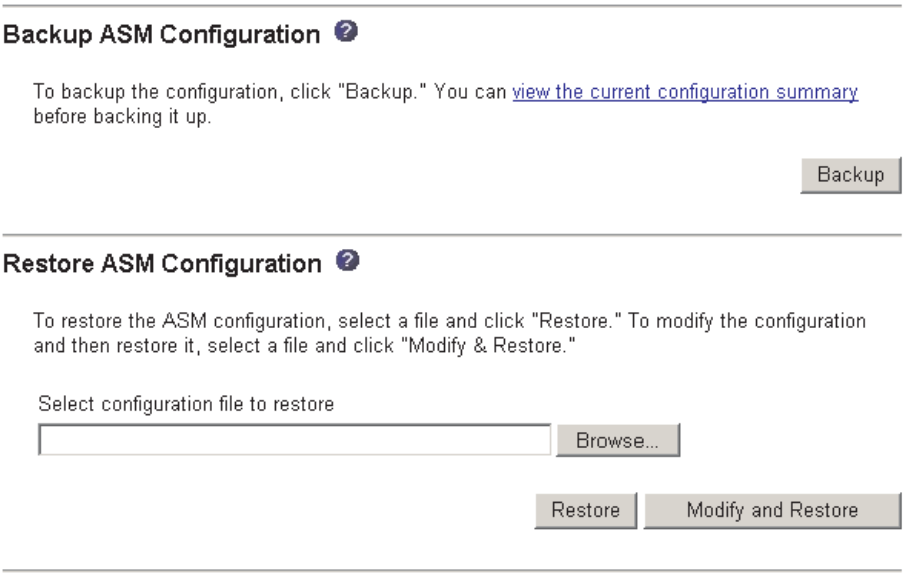
where *-x* indicates no X Window System forwarding and *-l* indicates that the session should use the user ID 'USERID'.

Using the configuration file

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

- Back up the ASM configuration
- Restore the ASM configuration

Important: Security page settings are not saved with the backup operation and cannot be restored with the restore operation.



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 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 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.

   Note: The security settings on the Security page are not restored with the restore operation. To modify security settings, see “Secure Web server and secure LDAP” on page 46.

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 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 35.

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

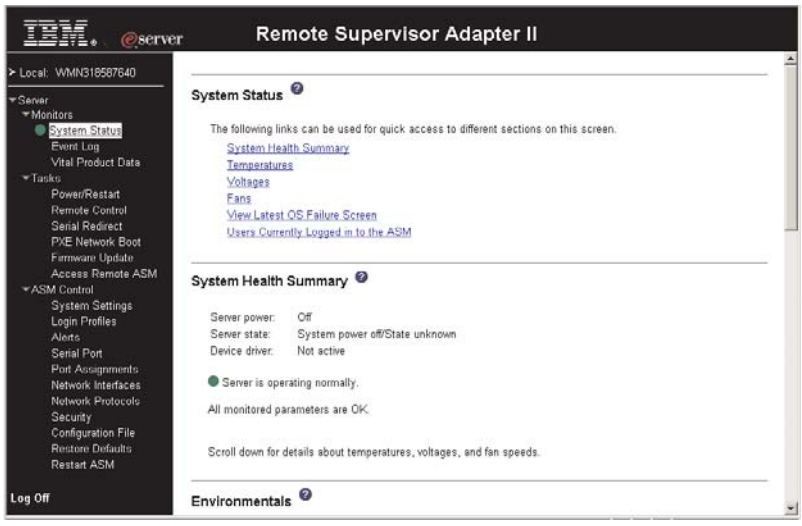
From the Vital Product Data (VPD) page, you can view the vital product data of the Remote Supervisor Adapter II, the server in which it is installed, and the ISMP.

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 interface,” on page 3.
2. In the navigation pane, click **System Status** 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:

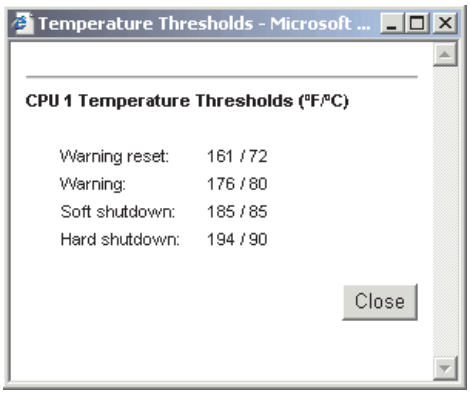
- A solid green circle and the phrase `Server is operating normally`

- 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 22.

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.

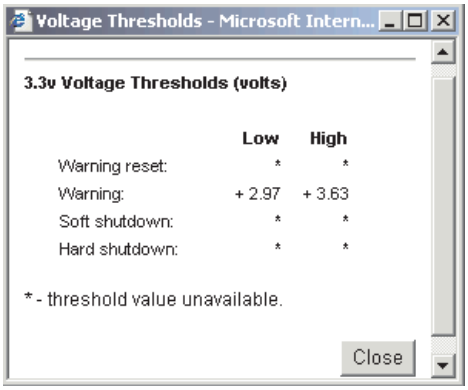
Hard Shutdown
: When the temperature reaches a specified value higher than the soft shutdown value (the hard shutdown threshold), the server immediately

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:

   1. To capture operating-system-failure screens, you must enable the OS Watchdog feature as described in “Setting server timeouts” on page 11.
   2. 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.

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:

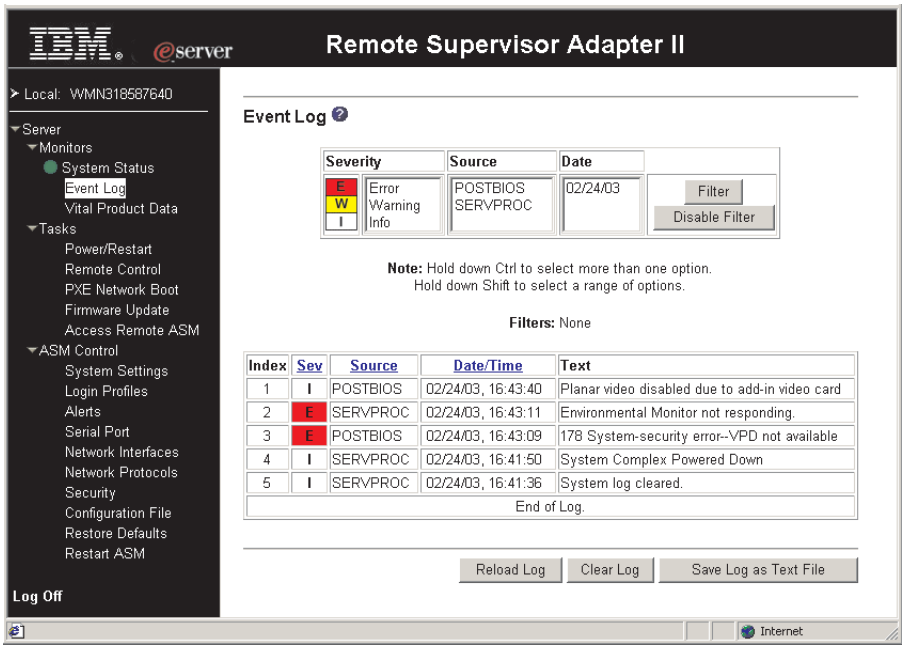
- Event log 75% full
- Event log full

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 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.



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.

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 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 11. 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 12. Component-level vital product data

Field	Function
FRU number	Identifies the field replaceable unit (FRU) number (a seven-digit alphanumeric identifier) for each component.

Table 12. Component-level vital product data (continued)

Field	Function
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 13. 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 14. 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 15. Diagnostics vital product data

Field	Function
Version	Indicates the version number of the diagnostic code.
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 16. 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 17. 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.

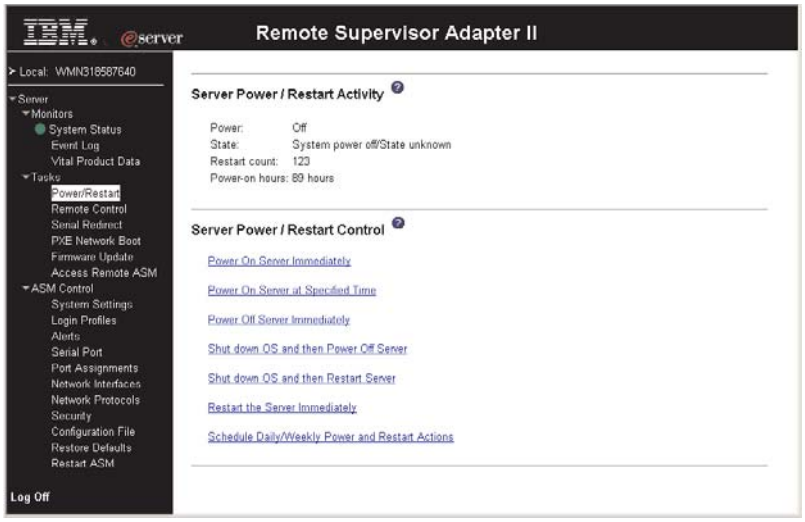
You can perform the following tasks:

- 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 Microsoft Windows 2000, Windows Server 2003, 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 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.

Important information about updating your Remote Supervisor Adapter II firmware

Important: If you have updated the Remote Supervisor Adapter II firmware to the latest level or plan to in the future, read the following information.

The Remote Supervisor Adapter II uses a Java applet to perform many functions. When the Remote Supervisor Adapter II is updated to the latest firmware level, the Java applet is also updated to the latest level. By default, Java caches (stores locally) applets that were previously used. After a flash update of the Remote Supervisor Adapter II firmware, the Java applet that the server uses might be downlevel.

Complete the following steps to correct this problem:

1. Click **Start → Settings → Control Panel**.
2. Double-click **Java Plug-in 1.4**. The **Java Plug-in Control Panel** window opens.

3. Click the **Cache** tab.
4. Choose one of the following options:
   - Clear the **Enable Caching** check box. If you choose this option, Java caching is always disabled.
   - Click **Clear Caching**. If you choose this option, you must click **Clear Caching** after each Remote Supervisor Adapter II firmware update.

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 interface,” on page 3.
2. In the navigation pane, click **Remote Control**. A page similar to the one in the following illustration is displayed.

3. To control the server remotely, use one of the links at the bottom of the Remote Control page. If you want exclusive remote access during your session, click **Start Remote Control in Single User Mode**. If you want to allow other users remote console (KVM) access during your session, click **Start Remote Control in Multi-user Mode**. A new window will open that provides access to the Remote Disk and Remote Console functionality.

   Note: The Remote Disk function does not support multiple users.

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

Notes:

1. Do not close the Remote Control window if a remote disk is currently mounted. See step 7 on page 77 for instructions for closing and unmounting a remote disk.
2. If you have mouse or keyboard problems when using Remote Control, see the help available from the Remote Control page in the Web interface.
3. 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

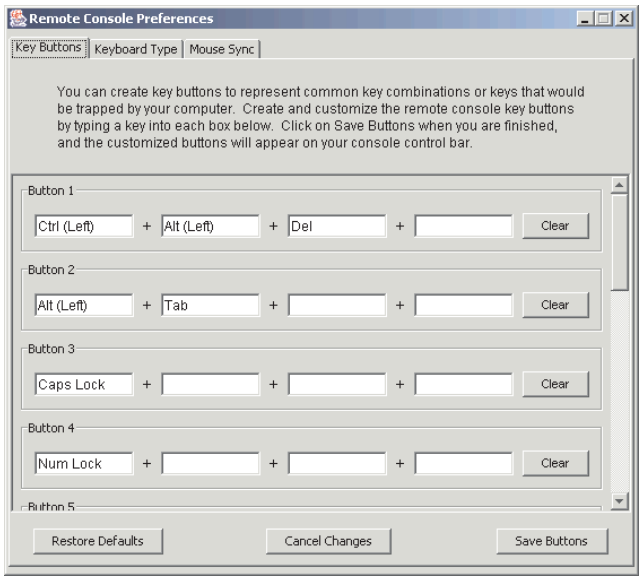
remote console and the login session. After a short delay, you can log in to the adapter again with a new session, start the remote console again, and exit the server Configuration/Setup Utility program.

Remote console keyboard support

The operating system on the client system you are using will trap certain key combinations, such as Ctrl+Alt+Del in Microsoft Windows, instead of transmitting them to the server. Other keys, such as F1, might cause an action on your computer as well as the server. Use the Remote Console **Preferences** link to create and edit customized buttons that can be used to send key strokes to the server.

Complete the following steps to create and edit customized buttons:

1. In the Remote Disk area, click **Preferences**.
2. Click the **Key Button** tab. A window similar to the one in the following illustration opens.



3. Follow the instructions on the Key Button tab and the other tabs.
4. Click **Save Buttons**.

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:

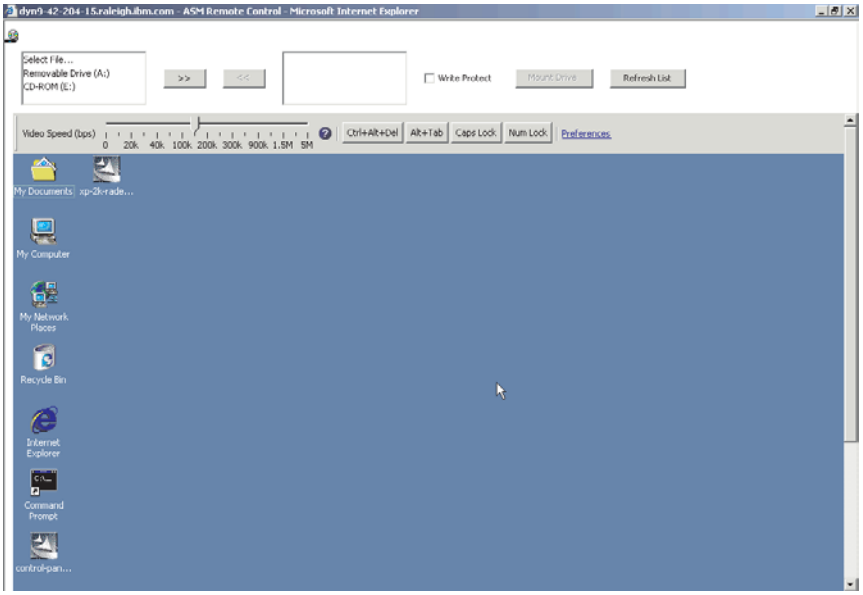
1. The following server operating systems have USB support, which is required for the Remote Disk feature:
   - Microsoft Windows Server 2003
   - Microsoft Windows 2000 with Service Pack 4 or later
   - Red Hat Linux version 7.3

- SuSE Linux version 8.0

2. The client system requires 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 interface,” on page 3.
2. In the navigation pane, click **Remote Control**.
3. In the Remote Control page, click one of the **Start Remote Control** options. A page similar to the one in the following illustration is displayed.



The Remote Control window contains the remote disk controls in the **Remote Disk** area at the top of the window. The Remote Control window also contains the server console in the **Remote Console** area (see “Remote console” on page 74).

4. To mount hard disk drives or disk images on the server, select the desired hard disk drives or images in the left-hand side of the Remote Disk drive selector, and use the >> button to move them to the right-hand side. Items can be removed from the right-hand side using the << button. When you click **Mount Drives**, the drives or images shown in the right-hand side will be mounted. Before mounting, click the **Write Protect** check box to prevent data being written to the mounted drives.

   When you select a diskette drive or an image file and move it to the right-hand side of the drive selector, you are given the option to save the disk image in the Remote Supervisor Adapter II random access memory (RAM). This will allow the disk image to remain mounted on the server and allow you to access the disk image later, even after the Web interface session is terminated. All other mounted drives will be unmounted when the Remote Control window is closed. A maximum of one drive or image can be stored on the Remote Supervisor Adapter II. The size of the drive or image contents must be 1.44 MB or smaller.

   Important: You will lose the disk image when the Remote Supervisor Adapter II is restarted or the Remote Supervisor Adapter II firmware is updated.

If the **Encrypt disk and KVM data during transmission** check box was selected before the Remote Control window was opened, the disk data is encrypted with 3DES encryption.

Note: The **Encrypt disk and KVM date during transmission** check box is not available on all servers.

To use the mounted disk, use the Remote Console function. The mounted disk will appear as a USB disk drive attached to the server.

5. 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.

6. Click **Mount Drive**. If you clicked **Select File** in step 5, 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.

7. 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**.

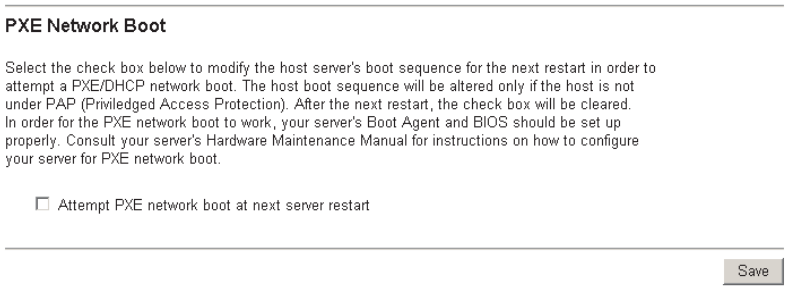
Setting up PXE network boot

Note: The PXE network boot feature is not available on all servers.

Complete the following steps to set up your server to attempt a Preboot Execution Environment (PXE) network boot at the next server restart:

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

2. In the navigation pane, click **PXE Network Boot**. A page similar to the one in the following illustration is displayed.



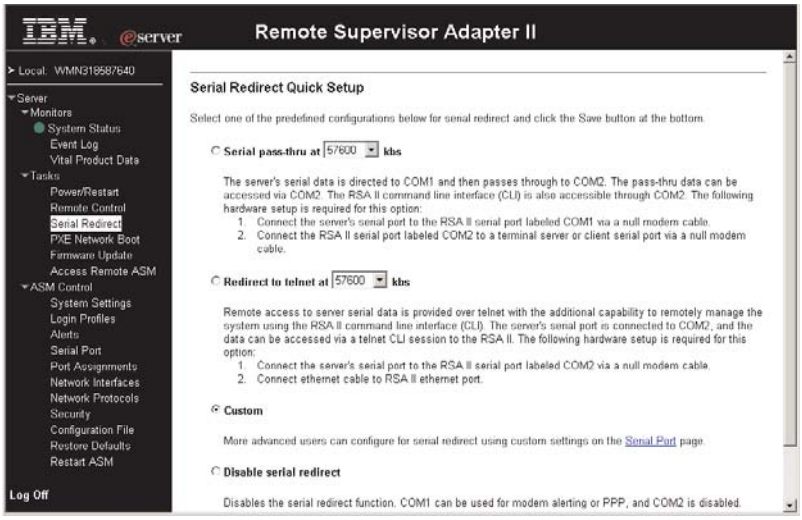
3. Click the **Attempt PXE network boot at next server restart** check box.
4. Click **Save**.

Serial redirection quick setup

You can use the Remote Supervisor Adapter II Web interface serial redirection wizard to simplify the configuration of serial redirection.

Complete the following steps to use the serial redirection wizard:

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



3. Use the following information to complete the quick setup information:

   Serial pass-thru

   The serial data of the server is directed to COM1 and then passes through to COM2. The pass-thru data can be accessed via COM2. The Remote Supervisor Adapter II command line interface (CLI) is also accessible through COM2. The following hardware setup is required for this option:

   - Connect the serial port of your server to the Remote Supervisor Adapter II serial port labeled COM1 using a null modem cable.
   - Connect the Remote Supervisor Adapter II serial port labeled COM2 to a terminal server or client serial port using a null modem cable.

Redirect to Telnet

Remote access to server serial data is provided over Telnet with the additional capability to remotely manage the system using the Remote Supervisor Adapter II command line interface (CLI). The server serial port is connected to COM2, and the data can be accessed using a Telnet CLI session to the Remote Supervisor Adapter II. The following hardware setup is required for this option:

- Connect the server serial port to the Remote Supervisor Adapter II serial port labeled COM2 using a null modem cable.
- Connect an Ethernet cable to the Remote Supervisor Adapter II Ethernet port.

Custom

Advanced users can configure for serial redirection using custom settings on the Serial Port page. To access the Serial Port settings page, click **Serial Port**.

Disable serial redirect

Disables the serial redirect function. COM1 can be used for modem alerting or PPP, and COM2 is disabled.

Updating firmware

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

Notes:

1. To update the firmware or operating system on the server remotely, see “Remote disk” on page 75.
2. If you plan to use the Remote Control feature after you update the firmware, see “Important information about updating your Remote Supervisor Adapter II firmware” on page 73.

Note:

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 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**.

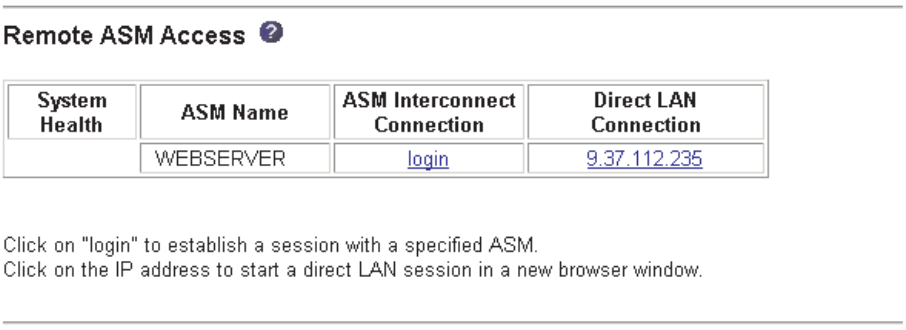
Accessing remote adapters through an ASM interconnect network

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 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.



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.ibmlink.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

Trademarks

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

e-business logo	Predictive Failure Analysis
@server	ServerGuide
IBM	ServerProven
IntelliStation	xSeries
IBM Global Network	

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

M

N

O

P

R

S

T

U

V

W

Part Number: 88P9267

Printed in USA

(1P) P/N: 88P9267