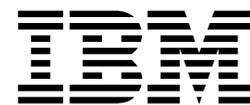
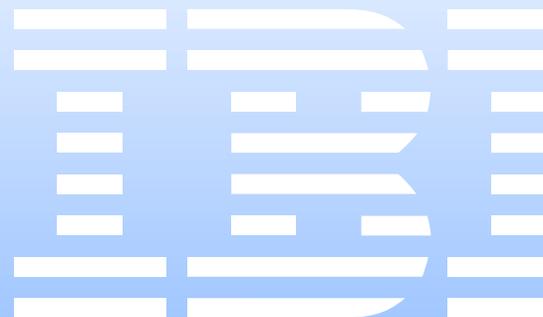


IBM Remote Supervisor Adapter

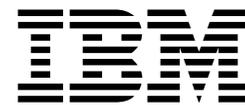


# User's Guide for the @server xSeries 360





IBM<sup>®</sup> Remote Supervisor Adapter



# User's Guide for the xSeries 360

**Note:** Before using this information and the product it supports, be sure to read the general information in Appendix B, "Notices," on page 95.

**First Edition (December 2001)**

**© Copyright International Business Machines Corporation 2001. All rights reserved.**

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

---

# Contents

|                                                                                   |    |
|-----------------------------------------------------------------------------------|----|
| <b>Chapter 1. Introduction</b> . . . . .                                          | 1  |
| Remote Supervisor Adapter features . . . . .                                      | 1  |
| Web browser requirements . . . . .                                                | 2  |
| Notices used in this book . . . . .                                               | 2  |
| <br>                                                                              |    |
| <b>Chapter 2. Opening and using the ASM Web interface</b> . . . . .               | 3  |
| <br>                                                                              |    |
| <b>Chapter 3. Using the Web-based interface</b> . . . . .                         | 7  |
| Monitoring the remote server status . . . . .                                     | 7  |
| Viewing the event log . . . . .                                                   | 10 |
| Viewing vital product data . . . . .                                              | 11 |
| <br>                                                                              |    |
| <b>Chapter 4. Performing Remote Supervisor Adapter tasks</b> . . . . .            | 15 |
| Server power and restart activity . . . . .                                       | 15 |
| Remotely controlling the power status of a server . . . . .                       | 16 |
| Remote control . . . . .                                                          | 17 |
| Accessing the server graphical console . . . . .                                  | 17 |
| Viewing the server POST . . . . .                                                 | 18 |
| Viewing the server blue screen . . . . .                                          | 18 |
| Changing the host server startup sequence . . . . .                               | 20 |
| Updating firmware . . . . .                                                       | 21 |
| Accessing remote adapters through an ASM interconnect network . . . . .           | 21 |
| <br>                                                                              |    |
| <b>Chapter 5. Configuring your Remote Supervisor Adapter</b> . . . . .            | 25 |
| Setting system information . . . . .                                              | 26 |
| Setting server timeouts . . . . .                                                 | 26 |
| Setting the ASM date and time . . . . .                                           | 29 |
| Creating a login profile . . . . .                                                | 30 |
| Setting the global login settings . . . . .                                       | 31 |
| Configuring remote alert settings . . . . .                                       | 32 |
| Setting remote alert attempts . . . . .                                           | 34 |
| Setting remote alerts . . . . .                                                   | 35 |
| Setting local events . . . . .                                                    | 37 |
| Configuring remote control keys . . . . .                                         | 38 |
| Configuring the serial port . . . . .                                             | 39 |
| Initialization-string guidelines . . . . .                                        | 42 |
| Configuring an Ethernet connection to ASM . . . . .                               | 42 |
| Configuring PPP access over a serial port . . . . .                               | 45 |
| Configuring SNMP . . . . .                                                        | 47 |
| Configuring SMTP . . . . .                                                        | 49 |
| Backing up your current configuration . . . . .                                   | 49 |
| Restoring your ASM configuration . . . . .                                        | 50 |
| Restoring a changed configuration . . . . .                                       | 50 |
| Restoring ASM defaults . . . . .                                                  | 51 |
| Restarting ASM . . . . .                                                          | 51 |
| Logging off . . . . .                                                             | 51 |
| <br>                                                                              |    |
| <b>Chapter 6. Starting and configuring the ASM text-based interface</b> . . . . . | 53 |
| Accessing a text-based interface via a TELNET connection . . . . .                | 53 |
| Accessing a text-based interface via a direct serial connection . . . . .         | 54 |
| Configuring terminal settings . . . . .                                           | 54 |
| <br>                                                                              |    |
| <b>Chapter 7. Configuring your Remote Supervisor Adapter using a text-based</b>   |    |

|                                                                                 |    |
|---------------------------------------------------------------------------------|----|
| <b>interface</b> .....                                                          | 57 |
| Setting system information .....                                                | 57 |
| Setting server timeouts .....                                                   | 58 |
| Creating a login profile .....                                                  | 61 |
| Setting modem and dial-in settings .....                                        | 63 |
| Configuring remote alert recipients .....                                       | 63 |
| Setting remote alert attempts .....                                             | 66 |
| Setting remote alerts .....                                                     | 67 |
| Configuring the serial port .....                                               | 70 |
| Initialization-string guidelines .....                                          | 72 |
| Configuring network interfaces .....                                            | 72 |
| Configuring an Ethernet connection to ASM .....                                 | 72 |
| Configuring PPP access over the serial port .....                               | 75 |
| Configuring network protocols .....                                             | 77 |
| Configuring SNMP .....                                                          | 77 |
| Configuring DNS .....                                                           | 78 |
| Configuring SMTP .....                                                          | 79 |
| Setting the Remote Supervisor Adapter clock .....                               | 80 |
| <br>                                                                            |    |
| <b>Chapter 8. The text-based Interfaced system health and tasks</b> .....       | 81 |
| Monitoring temperatures, voltage, and fan readings .....                        | 81 |
| Viewing the event log .....                                                     | 82 |
| Viewing vital product data .....                                                | 83 |
| Performing Remote Supervisor Adapter tasks through a text-based interface ..... | 85 |
| Remotely controlling the power status of a server .....                         | 86 |
| Accessing remote adapters through ASM interconnect network .....                | 86 |
| Viewing remote POST .....                                                       | 87 |
| Powering on or restarting servers .....                                         | 87 |
| Viewing the server text console .....                                           | 88 |
| Restoring ASM to factory defaults .....                                         | 88 |
| Restarting ASM .....                                                            | 89 |
| Logging off .....                                                               | 89 |
| <br>                                                                            |    |
| <b>Appendix A. Getting information, help, and service</b> .....                 | 91 |
| Getting information .....                                                       | 91 |
| Using the World Wide Web .....                                                  | 91 |
| Getting information by fax .....                                                | 91 |
| Getting help and service .....                                                  | 91 |
| Using the documentation and diagnostic programs .....                           | 91 |
| Calling for service .....                                                       | 92 |
| Telephone numbers .....                                                         | 93 |
| International Warranty Service .....                                            | 93 |
| Purchasing additional services .....                                            | 94 |
| <br>                                                                            |    |
| <b>Appendix B. Notices</b> .....                                                | 95 |
| Edition notice .....                                                            | 95 |
| Trademarks .....                                                                | 96 |
| <br>                                                                            |    |
| <b>Index</b> .....                                                              | 97 |

---

## Chapter 1. Introduction

This manual explains how to use the functions of the IBM® Remote Supervisor Adapter when you install it in an IBM @server xSeries 360. The IBM Remote Supervisor Adapter is one of the products in the Advanced System Management (ASM) family. The Remote Supervisor Adapter provides around-the-clock remote access and system management of your server and supports the following:

- Remote management independent of the status of the managed server
- Remote control of hardware and operating systems
- Web-based management with standard Web browsers (no other software is required)
- Text-based user interface

You can use either the ASM Web interface or the text-based interface to access the Remote Supervisor Adapter. This manual refers to either the ASM Web interface or the text-based interface for the Remote Supervisor Adapter, depending on the context.

---

### Remote Supervisor Adapter features

Standard features of the Remote Supervisor Adapter are as follows:

- Continuous health monitoring and control
- Automatic notification and alerts
- Battery-backed event log showing time-stamped entries
- Remote access through Ethernet, point-to-point protocol (PPP) connection, serial port, and ASM interconnect peer-to-peer network
- Simple Network Management Protocol (SNMP) traps
- E-mail alerts
- Alphanumeric or numeric pager alerts
- Domain Name System (DNS) server support
- Dynamic Host Configuration Protocol (DHCP) support
- Remote power control
- Blue screen capture
- Remote firmware update
- Access to critical server settings
- Text-based user interface terminal access
- Redirection of the server graphical or text console
- Access to server Vital Product Data (VPD)

---

## Web browser requirements

The ASM Web interface supports the following Web browsers:

- Microsoft® Internet Explorer version 4.0 (with Service Pack 1), or later
- Netscape Navigator version 4.72, or later (except version 6.0, which is not supported)

The ASM Web interface has the following browser-related requirements:

- Java™ enabled Web browser (see your browser documentation or online Help for instructions about enabling its Java support)
- JavaScript version 1.2, or later (see your browser documentation or online Help for instructions about enabling its JavaScript support)
- HTTP version 1.0, or later
- Minimum display resolution of 800 x 600 with 256 colors

**Note:** The ASM Web interface and the ASM text-based interface do not support the double byte character set (DBCS) languages.

---

## Notices used in this book

This book contains certain notices to highlight important information.

The notices and their definitions are:

- **Note:** 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 possible 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 ASM Web interface

Use the following procedure to access the Remote Supervisor Adapter through the ASM 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 to which you want to connect.

The Enter Network Password window opens.

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



Enter Network Password

Please type your user name and password.

Site: 9.67.41.147

Realm: Local System

User Name

Password

Save this password in your password list

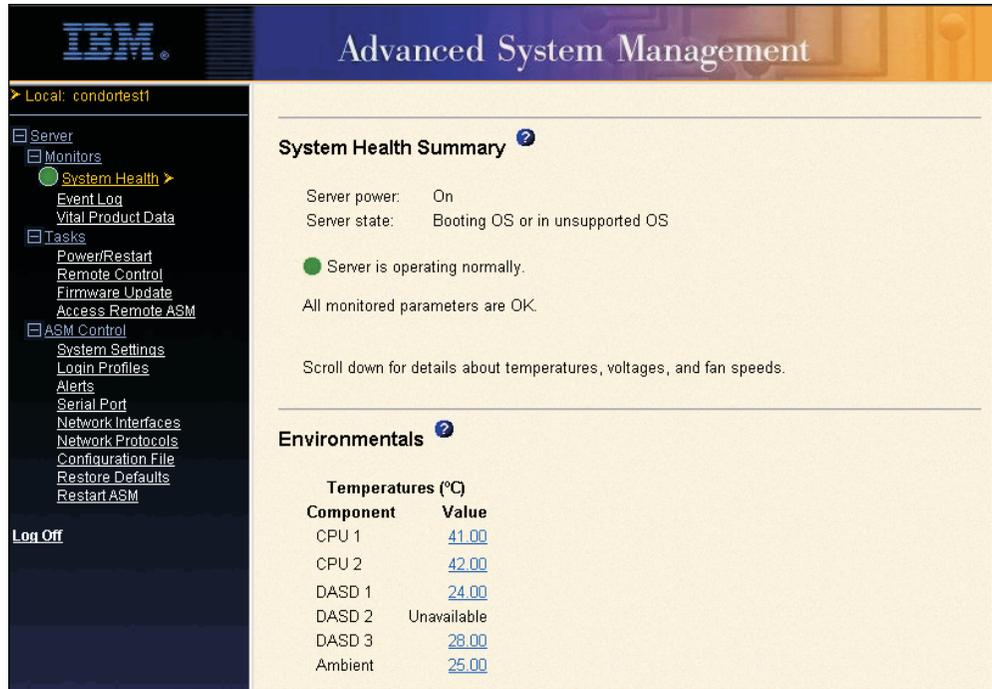
OK Cancel

2. Type your user name and password in the Enter Network Password window. If you are using the Remote Supervisor Adapter 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 is set initially with a user name of USERID and password of PASSWORD (with a zero, not an O). This user has read/write access. Change this default password during your initial configuration for enhanced security.

3. Select a timeout value, in minutes, in the field provided. If your browser is inactive for that number of minutes, the Remote Supervisor Adapter logs you off the Web interface.
4. Click **Continue** to start the session. The browser opens the System Health page, which gives you a quick view of the server status.

The following window displays the ASM Web interface showing the System Health home page.



The navigation frame of the ASM window contains the following navigational links that enable you to manipulate your Remote Supervisor Adapter or check the status of a server:

### System health

You can monitor the power and restart, temperature, voltage, and fan status of your server on the System Health Summary page. The System Health Summary page is the default homepage for the ASM Web interface. For more information on interpreting the system health summary data, see "Monitoring the remote server status" on page 7.

### Event log

The Event Log window contains entries that are currently stored in the system error log and POST error log. Information about all remote access attempts and dial-out events is recorded in the adapter event log. The Remote Supervisor Adapter time stamps all events and logs them into the event log, sending out the appropriate alerts if configured to do so by the system administrator. For more information on checking the event log, see "Viewing the event log" on page 10.

### Vital product data

Upon server startup, the Remote Supervisor Adapter collects system, BIOS, 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 server that the Remote Supervisor Adapter is monitoring. For more information on viewing vital product data, see "Viewing vital product data" on page 11.

### Power/restart

The Remote Supervisor Adapter 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. For more information on remote restarting, see “Remotely controlling the power status of a server” on page 16.

### **Remote control**

From the Remote Control page, you can:

- Redirect the server graphical OS desktop
- Redirect the server text console
- Restart the server and view the POST process
- View the image of the last Windows® blue screen capture

### **PXE Network Boot**

You can change the host server startup (boot) sequence for the next restart to attempt a PXE/DHCP network startup. For more information on changing the Preboot eXecution Environment (PXE) network startup sequence, see “Changing the host server startup sequence” on page 20.

### **Firmware update**

You can update firmware components on the Remote Supervisor Adapter and the server it monitors using the Firmware Update page. For more information on updating firmware, see “Updating firmware” on page 21.

### **Access remote ASM**

You can access other Remote Supervisor Adapters over the ASM interconnect network. This page displays a list of ASM processors, ASM PCI adapters, and Remote Supervisor Adapters present on the same ASM interconnect network, and enables you to establish a remote connection to any of those systems. For more information on remotely accessing the Remote Supervisor Adapter, see “Accessing remote adapters through an ASM interconnect network” on page 21.

### **System settings**

You can set general information (including the name for the Remote Supervisor Adapter), set contact information for the adapter, and set the server location. For more information on setting the system information section, see “Setting system information” on page 26.

### **Login profiles**

You can define twelve login profiles that enable access to the Remote Supervisor Adapter. For more information on defining login profiles, see “Creating a login profile” on page 30.

**Alerts** You can set the Remote Supervisor Adapter to provide alerts for a number of different situations. Click **Alerts** to set the standards for these alerts, including the remote alert recipients, number of alert attempts, incidents that trigger remote alerts, and local alerts. For more information on configuring remote alert recipients and the alerts to send, see “Setting remote alert attempts” on page 34 and “Setting remote alerts” on page 35.

### **Serial port**

You can set serial port baud rate and modem settings, and either dedicate the integrated serial port on the Remote Supervisor Adapter to system management or share it with the operating system. If dedicated to system management, the serial port is used by only the Remote Supervisor Adapter, and is always available for dial-in and dial-out alerting purposes. You will not be able to monitor the port from the Network Operating System (NOS) or from any other applications. For more information on dedicating the serial port, see “Configuring the serial port” on page 39.

### **Network interfaces**

You can configure the Remote Supervisor Adapter to have a remote access connection over an Ethernet connection or by point-to-point protocol (PPP). This enables remote access using a Web browser or TELNET application. For more information on setting up an Ethernet connection to the Remote

Supervisor Adapter, see “Configuring an Ethernet connection to ASM” on page 42. For more information on setting up a PPP using the serial port connection, see “Configuring PPP access over a serial port” on page 45.

### **Network protocols**

The Domain Name System (DNS) server setup is used to translate host names to IP addresses. The simple mail transfer protocol (SMTP) setup is used to configure the mail server for e-mail alerts. The SNMP setup enables you to define communities for sending SNMP traps and to configure SNMP agent settings. For more information on setting up the network protocols, see “Configuring SNMP” on page 47 and “Configuring SMTP” on page 49.

### **Remote control keys**

During server console redirect and remote POST, keyboard support is limited to ASCII characters, the arrow keys, and the F1 through F12 function keys. To transmit certain special key combinations, you must type the default prefix key combination or a user-defined prefix key combination. For more information on defining key combinations, see “Configuring remote control keys” on page 38.

### **Configuration files**

You can save the Remote Supervisor Adapter configuration on the remote administrator workstation, transfer it to another adapter, and edit it before restoring it on the adapter. With this function, you can deploy multiple managed systems without having to manually enter all the configuration data. For more information on saving and restoring the configuration, see “Restoring a changed configuration” on page 50.

### **Restore defaults**

**Attention:** When you click **Restore Defaults**, all of the modifications you made to the Remote Supervisor Adapter are lost.

You can reset the Remote Supervisor Adapter to its original factory settings. When you click the **Restore Defaults** button, you will lose your TCP/IP connection to that server and you must reconfigure the network interface locally using the configuration utility (or through the text-based user interface if serial port access is available).

For more information on restoring defaults, see “Restoring ASM defaults” on page 51.

### **Restart ASM**

You can restart the Remote Supervisor Adapter. For more information on restarting ASM, see “Restarting ASM” on page 51.

### **Log off**

You can log off from your connection to the Remote Supervisor Adapter with this option. For more information on logging off, see “Logging off” on page 51.

You can click the **View Configuration Summary** link, which appears on most pages, to quickly view how your Remote Supervisor Adapter is configured.

## Chapter 3. Using the Web-based interface

Use the links under the Monitors heading of the navigation frame to view the status of the server you access.

From the Event Log page, you can:

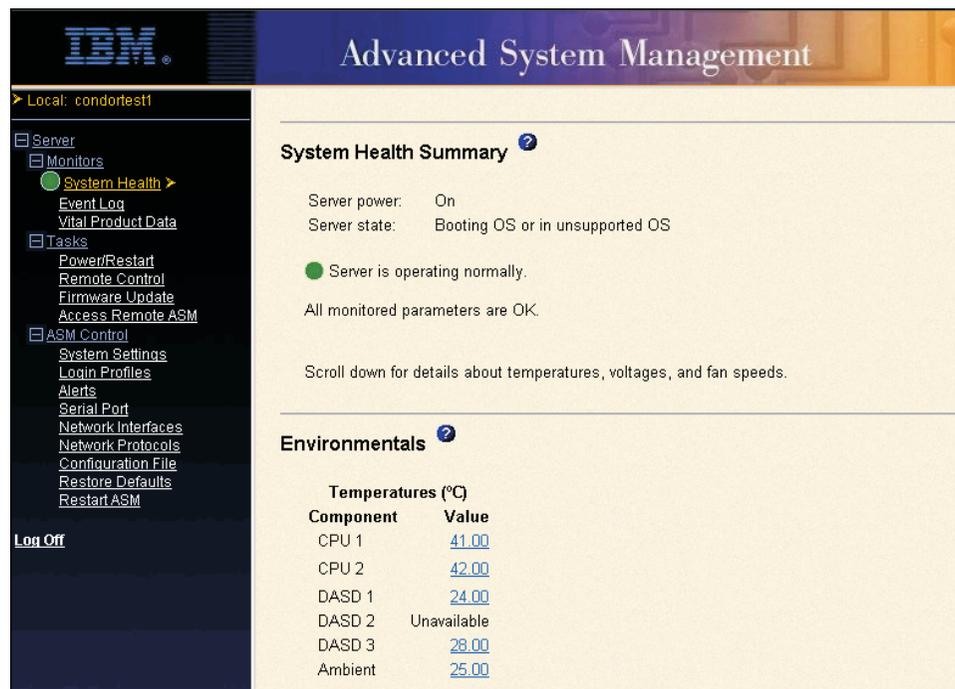
- View certain Advanced System Management events recorded in the Event Log of the Remote Supervisor Adapter
- View the severity of events

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

### Monitoring the remote server status

You can monitor the power and restart, temperature, voltage, and fan status of your server on the System Health Summary page. The System Health Summary page is the default home page for the ASM Web interface.

1. Log into the Remote Supervisor Adapter. For more information, see Chapter 2, “Opening and using the ASM Web interface,” on page 3.
2. In the navigation frame, click **System Health** to view a dynamically-generated update on the overall health of the server. A window similar to the following opens:



The screenshot displays the IBM Advanced System Management (ASM) web interface. The top navigation bar includes the IBM logo and the text "Advanced System Management". The left sidebar contains a navigation menu with categories like "Server", "Monitors", "Tasks", and "ASM Control". The "System Health" link is highlighted. The main content area shows the "System Health Summary" page, which includes a status indicator (a green circle) and text stating "Server is operating normally." and "All monitored parameters are OK." Below this, there is a section for "Environmentals" with a sub-section for "Temperatures (°C)". This section contains a table with two columns: "Component" and "Value".

| Component | Value       |
|-----------|-------------|
| CPU 1     | 41.00       |
| CPU 2     | 42.00       |
| DASD 1    | 24.00       |
| DASD 2    | Unavailable |
| DASD 3    | 28.00       |
| Ambient   | 25.00       |

The status of your server determines the message shown at the top of the System Health Summary page. One of the following 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 displays under one or both of the following:

- Critical events
  - Warnings and system events
3. Click Power/Restart to monitor the current power status of the system.

**Power** Indicates the power status of the server.

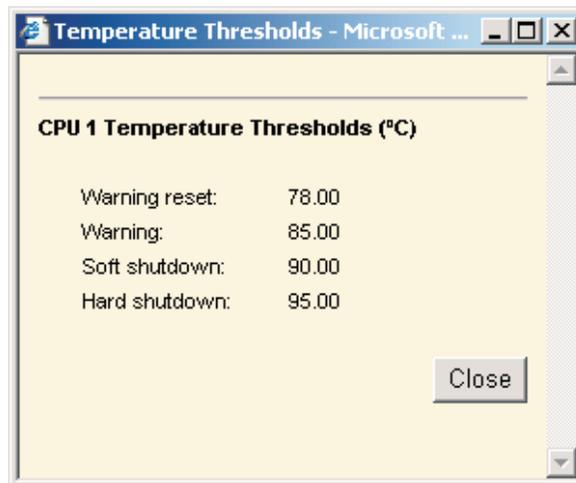
**State**

Displays the state of the operating system when this Web page was generated. Possible states include:

- System power off/State unknown
- In POST
- Stopped in POST (Error detected)
- Booted Flash or System partition
- Booting OS or in OS (Could be in the OS if the OS or application does not report the new system state.)
- In OS
- CPU’s held in reset

4. Scroll down to the temperatures section. The Remote Supervisor Adapter 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 following opens:



The Temperature Thresholds window displays the temperature levels at which the Remote Supervisor Adapter reacts. These levels are selected on the remote server and cannot be changed.

The reported temperature for the CPU, hard disk drive, and system is 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 will be generated.

### Warning

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

**Note:** For more information on selecting Alert options, see “Setting remote alerts” on page 35.

### Soft Shutdown

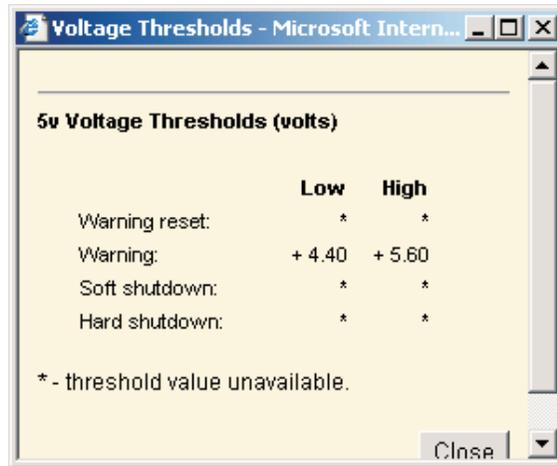
When the temperature reaches a specified value higher than the warning value (the soft shutdown threshold), a second temperature warning is sent to remote alert recipients and the server begins the shutdown process with an orderly operating system shutdown. The server then turns itself off. You must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

### Hard Shutdown

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

5. Scroll down to the voltages section. The Remote Supervisor Adapter 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 following opens:



The Voltage Thresholds window displays the voltage ranges at which the Remote Supervisor Adapter reacts. These levels are selected on the remote server and cannot be changed.

The ASM 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 generates no further alerts.

**Warning**

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

**Soft Shutdown**

When the voltage drops below or exceeds a specified voltage range, a voltage warning is sent to 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 option on the Alerts page for the warning to be sent.

**Hard Shutdown**

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

6. Scroll down to the Fan Speeds (percent of maximum) section. The ASM Web interface displays the running speed of the system fans (expressed in a percentage of the maximum fan speed). You receive a fan warning (Multiple Fan Failure or Single Fan Failure) when the fan speeds drop to an unacceptable level or stop. You must select the Fan options on the Alerts page for the warning to be sent.

---

## Viewing the event log

The Event Log window contains all entries that are currently stored in the remote managed server's error log and POST error log. Information about all remote access attempts and dial-out events is recorded in the adapter event log. The Remote Supervisor Adapter 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. Click the Save Log as Text File button to save the contents of the event log as a text file.

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

1. Log into the Remote Supervisor Adapter. For more information, see Chapter 2, "Opening and using the ASM Web interface," on page 3.
2. In the navigation frame, click **Event Log** to view the recent history of events on the server.
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 ASM Web interface distinguishes warning events with a yellow exclamation mark (!) in the severity column and error events with a red X.



## Viewing vital product data

Upon server startup, the Remote Supervisor Adapter collects system, basic input/output (BIOS), 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 is monitoring.

1. Log into the Remote Supervisor Adapter. For more information, see Chapter 2, "Opening and using the ASM Web interface," on page 3.
2. In the navigation frame, 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 VPD for the server appears in this section. For viewing VPD, the Machine VPD includes a Universally Unique Identifier (UUID).

**Note:** The Machine level VPD, Component level VPD, and component activity log will only provide information when the server is powered on.

Table 1. Machine level vital product data.

| Field         | Function                                                                                |
|---------------|-----------------------------------------------------------------------------------------|
| Machine type  | Identifies the type of server the Remote Supervisor Adapter is monitoring.              |
| Machine model | Identifies the model number of the server the Remote Supervisor Adapter is monitoring.  |
| Serial number | Identifies the serial number of the server the Remote Supervisor Adapter is monitoring. |
| UUID          | Identifies the Universally Unique Identifier (UUID), a 32-digit hexadecimal number.     |

### Component level VPD

The VPD for the components of the remote managed server appears in this section.

Table 2. Component level vital product data.

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

### POST/BIOS data

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 3. POST/BIOS vital product data.

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

### Power backplane data

You can find the VPD for the system power backplane firmware code in this section.

Table 4. Power Backplane vital product data.

| Field             | Function                                                        |
|-------------------|-----------------------------------------------------------------|
| Firmware revision | Identifies the revision number of the power backplane firmware. |

### Remote Supervisor Adapter system data

You can find the VPD for the Remote Supervisor Adapter in this section.

Table 5. Remote Supervisor Adapter vital product data.

| Field        | Function                                                                                                         |
|--------------|------------------------------------------------------------------------------------------------------------------|
| Build ID     | Identifies the build IDs and vital product data of the application firmware and the startup ROM firmware.        |
| Revision     | Identifies the revision numbers and vital product data of the application firmware and the startup ROM firmware. |
| File name    | Identifies the file names and vital product data of the application firmware and the startup ROM firmware.       |
| Release date | Identifies the release dates and vital product data of the application firmware and the startup ROM firmware.    |

### Integrated System Management Processor data

You can find the VPD for the integrated System Management processor firmware code in this section.

Table 6. Integrated System Management Processor vital product data.

| Field             | Function                                                                               |
|-------------------|----------------------------------------------------------------------------------------|
| Firmware revision | Identifies the revision number of the integrated System Management processor firmware. |

## Component Activity Log

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

Table 7. Component activity log.

| Field           | Function                                                                                                                                          |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| FRU number      | Identifies the field replaceable unit number (a seven-digit alphanumeric number) 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 activity log tracks the following server components:

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



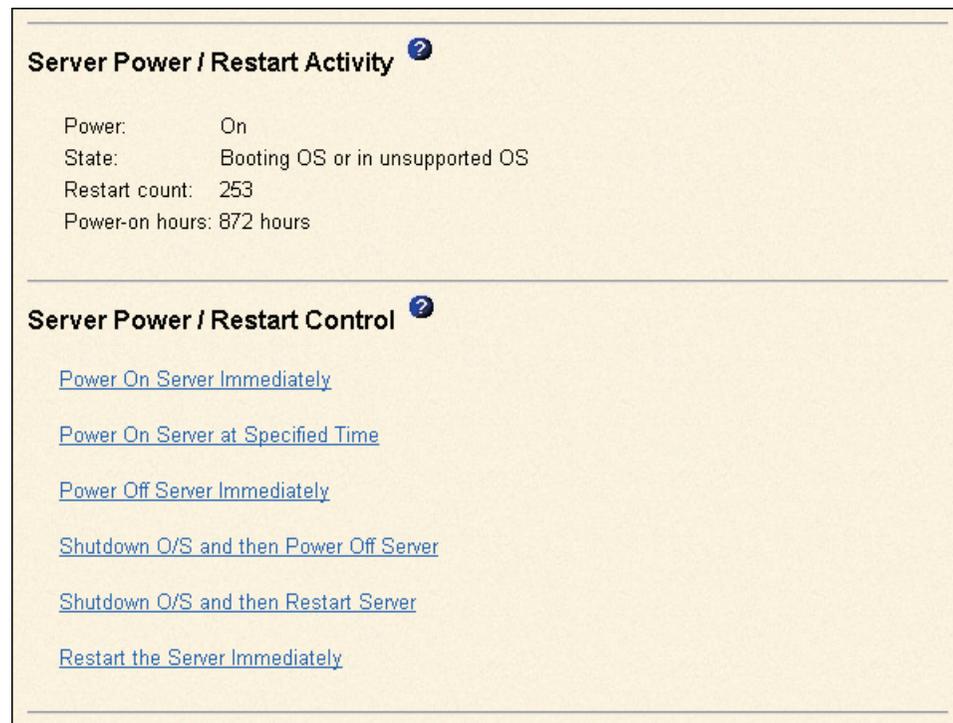
## Chapter 4. Performing Remote Supervisor Adapter tasks

The functions under the Tasks heading in the navigation frame enable you to directly control the actions of the Remote Supervisor Adapter and your server. You can perform the following tasks:

- View server power and restart activity
- Remotely control the power status of the server
- Access graphical remote console
- View server POST
- View remote blue screen capture
- Change the host server startup (boot) sequence
- Update firmware
- Access other Remote Supervisor Adapters

### Server power and restart activity

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



The screenshot shows a web interface with two main sections. The first section, titled "Server Power / Restart Activity", displays the following information: Power: On; State: Booting OS or in unsupported OS; Restart count: 253; Power-on hours: 872 hours. The second section, titled "Server Power / Restart Control", contains several blue hyperlinks: "Power On Server Immediately", "Power On Server at Specified Time", "Power Off Server Immediately", "Shutdown O/S and then Power Off Server", "Shutdown O/S and then Restart Server", and "Restart the Server Immediately".

**State** The State field shows the state of the system when this Web page was generated. Possible states include:

- 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
- CPU's held in reset
- System power on/Before POST

**Restart count**

The Restart count field shows the number of times the system 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 this server has been powered on.

## Remotely controlling the power status of a server

**Attention:** You must have the UM Server Extensions code installed to enable an orderly operating system shutdown. If you do not have the UM Server Extensions code installed, the server turns off after waiting for the length of time you set in the Power Off Delay field. You could lose or damage data on your server. For more information on installing UM Server Extensions code for the Remote Supervisor Adapter, see your *UM Server Extensions User's Guide*.

The Remote Supervisor Adapter 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.

**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 preschedule a server power on, click **Power On Server at Specified Time** to set the date and time.

**Power off server immediately**

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

**Shutdown O/S and then power off server**

To shut down the operating system and then turn off this server, click **Shutdown O/S and then Power Off Server**. This option requires that the Remote Supervisor Adapter device driver is installed on the server, as well as the agent component of IBM Director with UM Server Extensions.

**Shutdown O/S and then restart server**

To restart the operating system, click **Shutdown O/S and then Restart Server**. This option requires that the Remote Supervisor Adapter device driver is installed on the server, as well as the agent component of IBM Director with UM Server Extensions.

**Restart the server immediately**

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

A confirmation message displays if you select any of these options, enabling you to cancel the operation if it was selected accidentally.

To perform any of these actions, you must have read/write access to the Remote Supervisor Adapter. With the operating system shutdown options, the Remote Supervisor Adapter communicates with the system-management software through the device driver and the system-management software initiates the shutdown.

**Note:** For the operating system on the server to receive the shutdown notification from the Remote Supervisor Adapter, the server must have the IBM System Management device driver installed, as well as IBM Director with UM Server Extensions for the ASM component.

---

## Remote control

From the Remote Control page, you can:

- View the server graphical desktop image
- Restart the server and view the POST process in a TELNET window
- View the image of a Windows blue screen capture

You must log into the Remote Supervisor Adapter with a user ID that has read/write access to use any of the remote control features. You must also know the remote control password that is set on the remote server during BIOS code setup. After the password is accepted, you gain access to the server desktop. You do not need the remote control password to view the blue screen capture.

**Notes:**

1. You can have only one remote control session functioning at a time.
2. You have keyboard and mouse access to the server during text and graphical redirection, as well as during view POST operations.
3. The keystroke events sent by the remote client will not be received by 16-bit applications (for example, EDIT.COM or DEBUG.COM) running under Windows NT® or Windows 2000.

## Accessing the server graphical console

Click **Redirect Graphical Console** to view an interactive graphical user interface (GUI) display of the server. You see on your monitor exactly what you see on the server desktop, and you have keyboard and mouse control of the desktop.

**Notes:**

1. For best performance, set the server desktop to the following settings:
  - Supported resolutions: 640 x 480 pixels, 800 x 600 pixels (preferred), and 1024 x 768 pixels
  - Supported color depths: 256 colors, 65536 colors (preferred), and True Color
2. Some keyboard key combinations are not supported (such as Ctrl+Esc, Alt+Esc, and Alt+Tab).

**Note:** The Caps Lock, Scroll Lock, and Num Lock keys are not managed at the remote keyboard; they are managed by the server. When a connection is made on the remote keyboard, the state of these keys is irrelevant. The position of the keys at the server takes precedence. Pressing any of these keys on the remote keyboard after the connection is established will toggle both the LED on the remote keyboard and the Caps Lock, Scroll Lock, or Num Lock state at the server. However, the states never agree if they are different when the initial server connection is established.

3. Mouse control is supported on only the Windows NT and Windows 2000 operating systems.

4. If you switch the server to a full screen text-based display, the text-based information will not display in the redirected graphical console window. To remotely view the server text-based display, you must close the graphical console and start the text console.

Complete the following steps to remotely access a server graphical console:

1. Log into the Remote Supervisor Adapter. For more information, see Chapter 2, "Opening and using the ASM Web interface," on page 3.
2. In the navigation frame, click **Remote Control**.
3. Click **Redirect Graphical Console**. A Java™ applet opens in a separate browser window.
4. In the Password field, enter the remote control password. This password is configured locally on the server during the BIOS code update at the PAP field. For more information about the remote control password, see the *Remote Supervisor Adapter Installation Guide*.

The server desktop opens on your screen.

**Note:** For optimal viewing, set the resolution of the remote system to one setting smaller than the resolution of the monitor you will be viewing. For example, set the remote system resolution to 800 x 600 pixels if the monitor on which you are remotely viewing is set to 1024 x 768 pixels.

5. If a Microsoft Windows logon window opens, click **Send Ctrl+Alt+Del** to proceed. If the remote desktop is already displayed, use the mouse or the keyboard to navigate.

You can disconnect at any time by closing the applet windows.

## Viewing the server POST

Click **View Remote POST** to restart the server and view the POST within a TELNET window. You can interrupt the POST and access the server BIOS code run. You can view on your monitor what you can view on the server desktop, and you have keyboard control of the desktop.

The text-based interface view area is 80 characters x 24 lines.

Complete the following steps to remotely access a server POST:

1. Log into the Remote Supervisor Adapter. For more information, see Chapter 2, "Opening and using the ASM Web interface," on page 3.
2. In the navigation frame, click **Remote Control**.
3. To access the server POST, click the **View Remote POST**. A message is displayed, confirming that the server will be restarted.
4. Enter the remote control password. This password is configured on the server during BIOS code setup at the PAP field. For more information about the remote control password, see the *Remote Supervisor Adapter Installation Guide*.

A TELNET session opens, displaying the server text console on your screen.

You can disconnect at any time by closing the applet windows.

## Viewing the server blue screen

Click **View Windows Blue Screen** to access an image of the blue screen captured when the server stopped functioning. The blue-screen image shows the date and time of the capture. To capture a blue-screen event, you must enable the **O/S time out** option on the System page. You must be using Windows NT or Windows 2000 for this

feature to function. The Remote Supervisor Adapter stores only the latest blue-screen image.

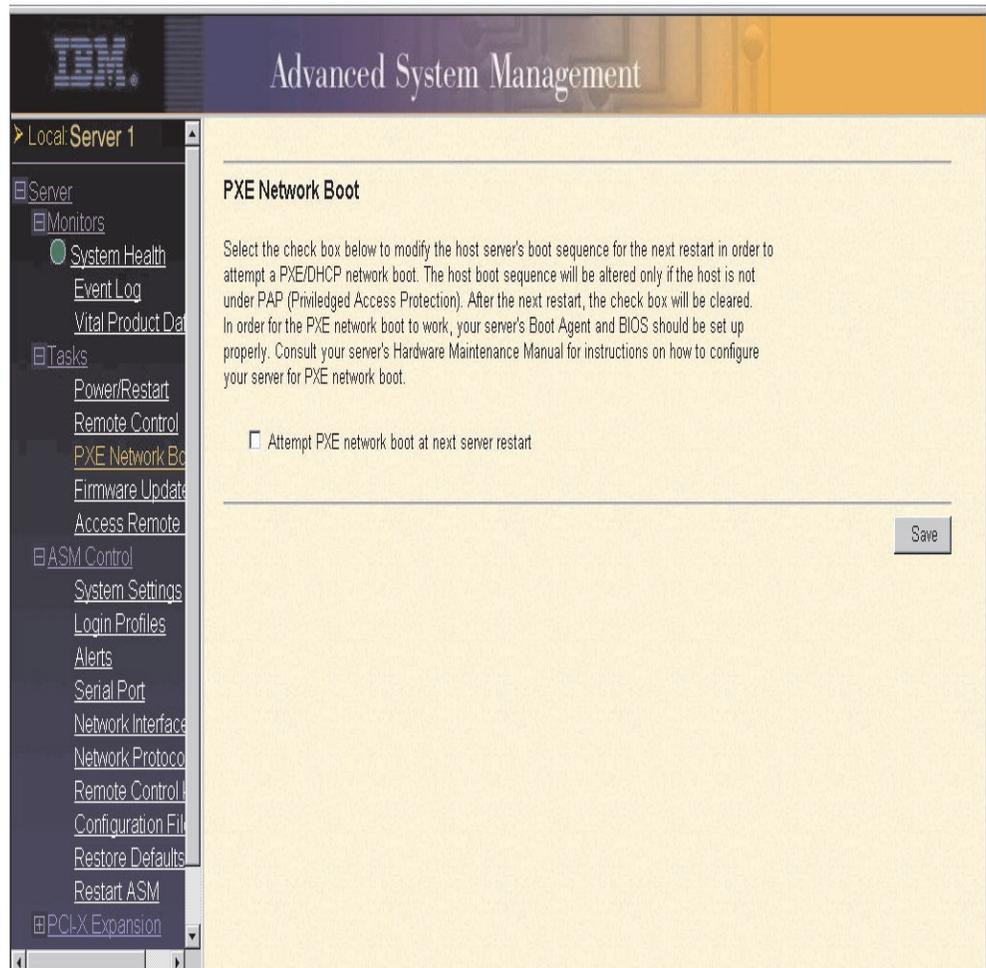
If a blue-screen event occurs while the operating system is up and running, and the server operating system stops running, the operating system timeout is triggered and causes the Remote Supervisor Adapter to capture the blue-screen data and store it. The image will not be overwritten during the next operating system install because the Remote Supervisor Adapter does not capture the operating system loader screen. Only error conditions are captured and maintained. The Remote Supervisor Adapter 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 blue-screen image:

1. Log into the Remote Supervisor Adapter. For more information, see Chapter 2, “Opening and using the ASM Web interface,” on page 3.
2. In the navigation frame, click **Remote Control**.
3. Click **View Windows Blue Screen**. The blue-screen image is displayed on your screen.

## Changing the host server startup sequence

If your server BIOS and PXE Boot Agent are properly defined, you can change the host server startup (boot) sequence for the next restart to attempt a PXE/DHCP network startup. To change the host server startup sequence, select the appropriate check box, as shown in the following illustration. 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 will be cleared.



---

## Updating firmware

Use the Firmware Update option on the navigation frame to update firmware of the Remote Supervisor Adapter or server.

Complete the following steps to update the startup or main application files of your Remote Supervisor Adapter. Updating firmware also enables BIOS code, diagnostics, power backplane, front panel, and serial peripheral interface (SPI) of the server in which the Remote Supervisor Adapter is installed, to be updated remotely using this function.

1. Log into the Remote Supervisor Adapter. For more information, see Chapter 2, “Opening and using the ASM Web interface,” on page 3.
2. In the navigation frame, 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. A confirmation page opens when the file transfer is completed.
7. Verify that the PKT or PKC file shown on the Confirm Firmware Update page is what you intend to update. If not, click the **Cancel** button.
8. To complete the update process, click **Continue**.  
A progress indicator opens as the firmware on the Remote Supervisor Adapter is flashed. A confirmation page opens to verify that the update was successful.
9. After receiving a confirmation that the update process is complete, go to the Restart ASM page and click **Restart**.
10. Click **OK** to confirm that you want to restart the Remote Supervisor Adapter.
11. Click **OK** to close the current browser window.
12. To log into the Remote Supervisor Adapter again, open your browser and follow your regular login process.  
**Note:** To cancel this process at any point, click **Cancel**.

---

## Accessing remote adapters through an ASM interconnect network

You can connect to remote systems through the ASM interconnect network on the Access Remote ASM page. 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 column provides a login link that enables you to quickly access each remote system.

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

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

2. In the navigation frame, click **Access Remote ASM**. The Remote Access ASM table appears, listing processors and adapters linked to the host server. The table also displays:

**System Health**

The system health icon of the remote ASM displays in this column.

**ASM Name**

The name of the remote ASM displays in this column.

**ASM Interconnect Connection**

The ASM Interconnect Connection column provides a login link that enables you to quickly access each remote system through the ASM interconnect network.

To log into 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 into a remote system displayed in the table, click on 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. The specific reason will be shown as one of the following:

**no LAN support**

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

**function not supported**

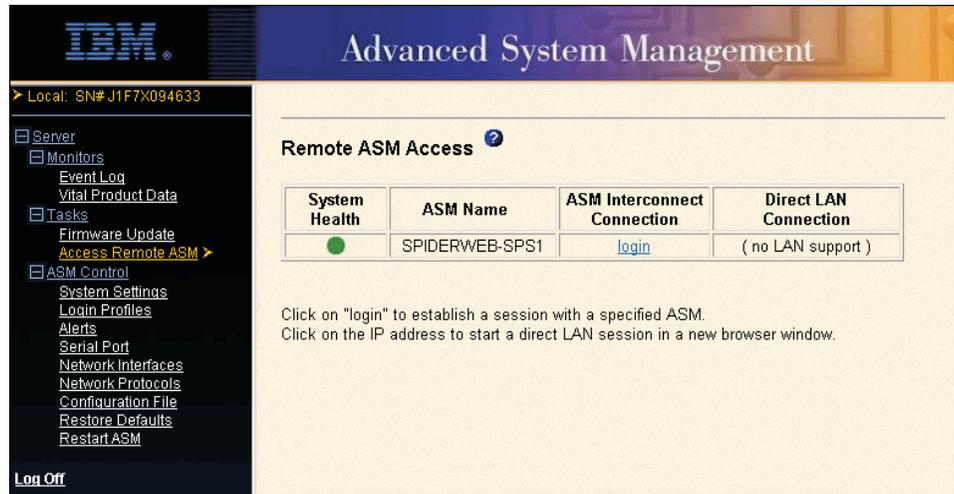
The system-management adapter of the remote system does not have the ability to report its IP address through the ASM interconnect network.

**no LAN connection**

The system-management processor or adapter of the remote system either:

- Has not been manually configured with an IP address
- Failed to receive a dynamic IP address assignment from a DHCP server
- Has a faulty physical LAN connection

A window similar to the following opens:



3. 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 two minutes for servers to be removed from the table when detached from the ASM interconnect network.

The Enter Network Password window opens.

4. Type your user name and password. The ASM window opens. The adapter or processor name appears in orange above the navigation frame.

**Note:** Depending on the system-management processor or adapter that is on the remote server, some options might not be available.



---

## Chapter 5. Configuring your Remote Supervisor Adapter

Use the links under the ASM Control heading in the navigation frame to configure your Remote Supervisor Adapter.

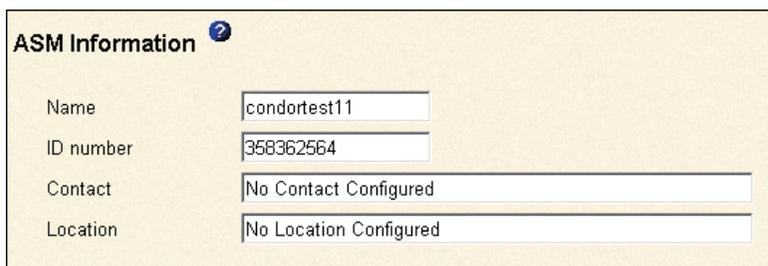
- From the System page, you can:
  - Set system information
  - Set server timeouts
  - Set ASM date and time
- From the Login Profiles page, you can:
  - Set login profiles to control access
  - Configure modem and dial-in settings
- From the Alerts page, you can:
  - Configure remote alert recipients
  - Set the number of remote alert attempts
  - Select the delay between alerts
  - Select which alerts will be sent and how they will be forwarded
- From the Serial Port page, you can:
  - Configure the serial port
  - Configure advanced modem settings
- From the Network Interfaces page, you can:
  - Set up an Ethernet connection
  - Set up a PPP over serial port connection
- From the Network Protocols page, you can:
  - Configure SNMP setup
  - Configure DNS setup
  - Configure SMTP setup
- From the Configuration File page, you can backup, modify, and restore the configuration of the Remote Supervisor Adapter.
- From the Restore Defaults page, you can reset the Remote Supervisor Adapter configuration to the factory defaults.
- From the Remote Control Keys page, you can configure key combinations.
- From the Restart ASM page, you can restart the Remote Supervisor Adapter.

---

## Setting system information

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

1. Log into the Remote Supervisor Adapter where you want to set the system information. For more information, see Chapter 2, “Opening and using the ASM Web interface,” on page 3.
2. In the navigation frame, click **System Settings**. A window similar to the following opens:



The screenshot shows a window titled "ASM Information" with a help icon. It contains four input fields:

|           |                        |
|-----------|------------------------|
| Name      | condortest11           |
| ID number | 358362564              |
| Contact   | No Contact Configured  |
| Location  | No Location Configured |

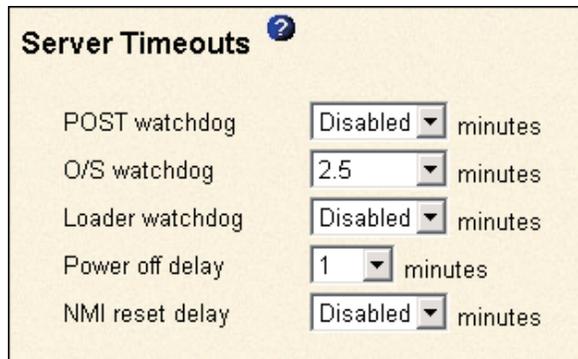
3. In the Name field, type the name of the Remote Supervisor Adapter.  
Use the Name field to specify a name for the Remote Supervisor Adapter in this server. The name is included with e-mail, SNMP, and alphanumeric pager alert notifications to identify the source of the alert.  
**Note:** Your Remote Supervisor Adapter name (the Name field) and the IP host name of the Remote Supervisor Adapter (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 consist of up to 63 characters. To minimize confusion, set the ASM Name field to the non-qualified portion of the IP host name. The non-qualified IP host name consists of up to the first period of a fully qualified IP host name. For example, the non-qualified IP host name of `asmcard1.us.company.com` (a fully qualified IP host name) is `asmcard1`. For more information on your host name, see “Configuring an Ethernet connection to ASM” on page 42.
4. In the ID number field, assign the Remote Supervisor Adapter 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.

## Setting server timeouts

Complete the following steps to set your server time-out values:

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

A window similar to the following is displayed:



| Setting         | Value    | Unit    |
|-----------------|----------|---------|
| POST watchdog   | Disabled | minutes |
| O/S watchdog    | 2.5      | minutes |
| Loader watchdog | Disabled | minutes |
| Power off delay | 1        | minutes |
| NMI reset delay | Disabled | minutes |

You can set the Remote Supervisor Adapter 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
  - Non-maskable interrupt
3. Enable the server timeouts that correspond to the events you want the Remote Supervisor Adapter to respond to automatically.

#### POST watchdog

Use the POST watchdog field to specify the number of minutes that the Remote Supervisor Adapter will wait for this 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 generates a POST time-out alert and restarts the server. The POST watchdog is then disabled until the operating system is shut down and the server is power-cycled (or until the operating system and device drivers successfully load).

**Note:** Power-cycling differs from shutting down and restarting the operating system in that power-cycling removes power from the server completely. For example, unplugging your server.

To set the POST time-out 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 attempts to forward the alert to all enabled 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 will be ignored.

Refer to your server documentation for further details.

#### 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. If the operating system fails to respond to one of these checks, the Remote Supervisor Adapter generates an O/S time-out 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 blue screens, you must enable this field and check the **O/S Time-out** check box in the Remote Alerts section of the Alerts page.

**Notes:**

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

**Loader watchdog**

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

To set the loader time-out value, select the time limit that the Remote Supervisor Adapter will wait for the operating system to load. To turn off this watchdog, select **Disabled**.

**Note:** If the **Loader Time-out** check box is selected in the Remote Alerts section of the Alerts page, the Remote Supervisor Adapter will send an alert to all enabled remote alert recipients.

**Power off delay**

Use the Power off delay field to specify how long the Remote Supervisor Adapter will wait for the operating system to shut down before turning off the system. By default, the Remote Supervisor Adapter waits 30 seconds.

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.

**Attention:** You must have the IBM Director with UM Server Extensions agent code installed to enable an orderly operating system shutdown. Even with this code installed, you could lose or corrupt data on your server. For more information on installing UM Server Extensions code for the Remote Supervisor Adapter, see the *UM Server Extensions User's Guide*. In order for the operating system to receive the shutdown notification from the Remote Supervisor Adapter, the server must have the Advanced System Management device driver and the ASM component of UM Server Extensions installed.

**NMI reset delay**

Use this field to specify the length of time in minutes that the ASM subsystem waits to automatically restart the server after a non-maskable interrupt (NMI) is triggered. A non-maskable interrupt usually indicates a critical error such as a hardware fault. A non-maskable interrupt usually signals a parity error in the memory subsystem.

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

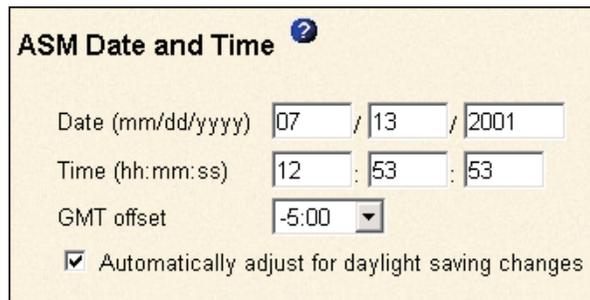
To set the NMI reset delay value, click the pull-down button and select the desired number of minutes. To disable the automatic server restart after a non-maskable interrupt, select **Disabled**.

## Setting the ASM date and time

The Remote Supervisor Adapter includes its own real-time clock to independently time-stamp all events that are logged in the battery-backed 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 savings time (DST) for added ease-of-use for administrators managing systems remotely over different time zones. You can remotely access the battery-backed event log even if the system is turned off or disabled. This facilitates immediate problem determination and resolution.

Complete the following steps to check the date and time processor settings on the Remote Supervisor Adapter, which is independent of the date and time settings of the clock on the server system board:

1. Log into the Remote Supervisor Adapter where you want to set the ASM date and time values. For more information, see Chapter 2, "Opening and using the ASM Web interface," on page 3.
2. In the navigation frame, click **System Settings** and scroll down to the ASM Date and Time section, which shows the date and time when this Web page was generated. A window similar to the following is displayed:



The screenshot shows a web form titled "ASM Date and Time" with a help icon. It contains the following fields:

- Date (mm/dd/yyyy): 07 / 13 / 2001
- Time (hh:mm:ss): 12 : 53 : 53
- GMT offset: -5:00 (dropdown menu)
- Automatically adjust for daylight saving changes

### Automatic Daylight Savings Time Update

Use the Automatically adjust for daylight saving changes check box to specify whether the Remote Supervisor Adapter clock will automatically adjust when DST changes.

### GMT offset

Use the GMT offset field to specify the offset from GMT corresponding to the time zone where this server is located.

To set the Time field, type the numbers corresponding to the current hour, minutes, and seconds in the appropriate text boxes. 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.

To override the date and time settings, and to enable DST and GMT, click **Set ASM Date and Time**.

To set the **Date**, type the numbers of the current month, day, and year in the matching text boxes.

3. Click **Save**.

## Creating a login profile

Complete the following steps to configure a login profile:

1. Log into the Remote Supervisor Adapter where you want to create a login profile. For more information, see Chapter 2, "Opening and using the ASM Web interface," on page 3.
2. In the navigation frame, click **Login Profiles**. The Login Profiles window displays the login ID and the login access level. A window similar to the following opens:

| Login ID                         | Access     |
|----------------------------------|------------|
| 1. <a href="#">USERID</a>        | Read/Write |
| 2. <a href="#">H</a>             | Read/Write |
| 3. <a href="#">~ not used ~</a>  |            |
| 4. <a href="#">~ not used ~</a>  |            |
| 5. <a href="#">~ not used ~</a>  |            |
| 6. <a href="#">~ not used ~</a>  |            |
| 7. <a href="#">~ not used ~</a>  |            |
| 8. <a href="#">~ not used ~</a>  |            |
| 9. <a href="#">~ not used ~</a>  |            |
| 10. <a href="#">~ not used ~</a> |            |
| 11. <a href="#">~ not used ~</a> |            |
| 12. <a href="#">~ not used ~</a> |            |

Use this page to view, configure, or change individual login profiles. You can define up to twelve unique profiles. If you did not configure a profile, the name of the profile link by default is ~ not used ~.

3. Click one of the unused login profile links. An individual profile page similar to the following opens:

|                  |                                         |
|------------------|-----------------------------------------|
| Login ID         | <input type="text" value="Jones"/>      |
| Authority level  | <input type="text" value="Read/Write"/> |
| Password         | <input type="password" value="****"/>   |
| Confirm password | <input type="password" value="****"/>   |
| Dialback status  | <input type="text" value="Disabled"/>   |
| Dialback number  | <input type="text"/>                    |

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.

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

**Read Only**

The Read Only option enables the user to view a page, but not to make changes. Additionally, people who log in with read-only IDs are unable to perform file transfers, power and restart actions, or remote control functions.

**Read/Write**

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

6. In the Password field, assign a password to the Login ID.  
Valid passwords must contain at least five characters, one of which must be a non alphabetic 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.
7. In the Confirm Password field, type the password again.
8. In the Status field of the Dialback Settings option, select **Enabled** or **Disabled** to configure the Remote Supervisor Adapter to automatically terminate a successful dial-in attempt and then immediately dial-out to a specified number.  
**Note:** If this menu is enabled, you must enter a phone number in the Number field of this profile.
9. In the Dialback number field, type the phone number that the Remote Supervisor Adapter will use when dialing-back to reach the login ID.  
This phone number is dialed when this user successfully logs into the Remote Supervisor Adapter.  
**Note:** By default, the Remote Supervisor Adapter is configured with one login profile that enables remote access using a login user ID of USERID and a password of PASSWORD (the 0 is a zero). To avoid a potential security exposure, change this default login profile during initial setup of the Remote Supervisor Adapter.
10. Click **Save** to save your login ID settings.

---

## Setting the global login settings

Complete the following steps to enable your modem to dial out to the remote login profile:

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

## Configuring remote alert settings

You can configure remote alert recipients, the number of alert attempts, incidents that trigger remote alerts, and local alerts. Use these remote alert recipient links to view, configure, or change individual alert recipients. You can define up to twelve unique recipients. Each link for an alert recipient is labeled with the recipient name, notification method, and alert status.

When you configure a remote alert entry, the Remote Supervisor Adapter will send an alert to a remote system (through a serial connection or a network connection, a numeric pager, or an alphanumeric pager) when any event selected from the Enabled Alerts group occurs. This alert will contain 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 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.

If the SNMP Agent or SNMP Traps fields are not enabled, no SNMP type alerts will be sent. For more information on these fields, see “Configuring SNMP” on page 47.

**Note:** You cannot distinguish between what alerts will be sent to which remote alert recipient. All configured recipients receive each alert you select.

Complete the following steps to configure a remote alert recipient:

1. Log into the Remote Supervisor Adapter for which you want to configure remote alert settings. For more information, see Chapter 2, “Opening and using the ASM Web interface,” on page 3.
2. In the navigation frame, click **Alerts**. The Remote Alert Recipients window appears. You can see the notification method and alert status, if set, for each recipient. A window similar to the following opens:

**Remote Alert Recipients** ⓘ

To configure a remote alert recipient, click a link in the "Name" column.

| Name                             | Notification Method | Status                        |
|----------------------------------|---------------------|-------------------------------|
| 1. <a href="#">H</a>             | E-mail over LAN     | Receives critical alerts only |
| 2. <a href="#">~ not used ~</a>  |                     |                               |
| 3. <a href="#">~ not used ~</a>  |                     |                               |
| 4. <a href="#">~ not used ~</a>  |                     |                               |
| 5. <a href="#">~ not used ~</a>  |                     |                               |
| 6. <a href="#">~ not used ~</a>  |                     |                               |
| 7. <a href="#">~ not used ~</a>  |                     |                               |
| 8. <a href="#">~ not used ~</a>  |                     |                               |
| 9. <a href="#">~ not used ~</a>  |                     |                               |
| 10. <a href="#">~ not used ~</a> |                     |                               |
| 11. <a href="#">~ not used ~</a> |                     |                               |
| 12. <a href="#">~ not used ~</a> |                     |                               |

Generate Test Alert

3. Click one of the remote alert recipient links. An individual recipient page similar to the following opens:

**Remote Alert Recipient 1**

Receives critical alerts only

Status: Enabled

Name: Jones

Notification method: E-mail over LAN

Number:

PIN:

E-mail address (userid@hostname): userid@computers

PPP login ID:

PPP password:

Reset to Defaults Cancel Save

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**.
6. In the **Name** field, type the name of the recipient or other identifier. The name you enter appears as the link for the recipient on the Alerts page.
7. In the **Notification method** field, select the notification method for reaching the recipient. Select one of the following notification methods:

- Numeric pager
- Alphanumeric pager
- IBM Director over Modem
- IBM Director over LAN
- SNMP over LAN
- E-mail over LAN
- SNMP over PPP
- E-mail over PPP

**Note:** If you select to send remote alerts by the IBM Director over Modem or IBM Director over LAN options, you must have UM Server Extensions installed on the IBM Director server.

8. In the **Number** field, type either the phone number, IP address, or host name at which to reach 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
- SNMP over PPP
- E-mail over PPP

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 or E-mail over PPP notification methods, in the E-Mail address field, type the e-mail address of the recipient.  
**Note:** For the E-mail over LAN and E-mail over PPP notification methods 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 49.
11. If you selected the E-mail over PPP or SNMP over PPP notification methods, at the PPP Login ID field, type the PPP login ID needed to log into the dial-up service account of the recipient. The PPP login ID consists of your service, your account name, and your user ID all separated by periods (service.account.userid).  
 For example, to log into the IBM Global Network IP Remote Access Service Provider, the PPP login ID should contain information in the following format: *secureip.X.Y*, where *secureip* is your service and *X* is your account name, and *Y* is your user ID.  
**Note:** For the SNMP over LAN and SNMP over PPP notification methods to work properly, configure the SNMP options on the Network Protocols page. For more information on SNMP, see “Configuring SNMP” on page 47.
12. If you selected the E-mail over PPP or SNMP over PPP notification methods, at the PPP password field, type the PPP password that accompanies the login ID.
13. Click **Save** to save your remote alert recipient profile. Repeat steps 3 through 11 for each remote alert recipient profile.
14. Click **Generate Test Alert** on the Remote Alert Recipients page to send a test alert to all enabled alert recipients.  
**Note:** All selected alert events are sent to all enabled alert recipients.

Continue with the “Setting remote alerts” on page 35 procedure.

## Setting remote alert attempts

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

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

**Global Remote Alert Settings** ?

Remote alert retry limit  times

Delay between retries  minutes

Use these settings to define the number of remote alert attempts and the 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 will attempt to send an alert to a recipient.

### Delay between retries

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

3. Select the **Include Event Log With E-mail Alerts** check box in the E-Mail Attachments section to attach the local event log to all e-mail alert notifications. The event log provides a summary of the most recent events and assists with problem identification and fast recovery.

### Notes:

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

Continue with the “Setting remote alerts” procedure.

## Setting remote alerts

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

1. Log into the Remote Supervisor Adapter where you want to set remote alerts. For more information, see Chapter 2, “Opening and using the ASM Web interface,” on page 3.
2. In the navigation frame, select **Alerts** and scroll down to the Monitored Alerts section.
3. Select the events you want the Remote Supervisor Adapter 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. The **Select all critical alerts** check box enables you to have an alert sent for any critical alert.

Table 8. Critical remote alerts.

| Event                   | Action                                                                        | Numeric code |
|-------------------------|-------------------------------------------------------------------------------|--------------|
| Hard disk drive failure | Generates an alert if one or more of the hard disk drives in the system fail. | 05           |
| Multiple fan failure    | Generates an alert if two or more of the cooling fans in the system fail.     | 03           |
| Power failure           | Generates an alert if any of the system power supplies fail.                  | 04           |

Table 8. Critical remote alerts.

| Event                    | Action                                                                                                                                                                                                                                                                                                                                                  | Numeric code |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| 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.                                                                                                                                                                                      | 02           |
| Temperature irregularity | Generates an alert if any of the monitored temperatures are outside critical threshold values. These threshold values can be found by clicking the temperature readings on the System Health page. If a critical temperature condition is detected, the server will shut down and turn off whether this field is selected or not.                       | 00           |
| Voltage irregularity     | Generates an alert if the voltages of any of the monitored power supplies fall outside their specified operational ranges. These operational ranges are accessed by clicking the voltage readings on the System Health page. If a critical voltage condition is detected, the server will shut down and turn off whether this field is selected or not. | 01           |
| VRM failure              | Generates an alert if one or more VRMs fail. VRMs are not used on some servers, in which case this setting is ignored.                                                                                                                                                                                                                                  | 06           |

### Warning alerts

Warning alerts are generated for events that might progress to a critical/error level. The **Select all warning alerts** check box enables you to have an alert sent for any warning alert.

Table 9. Warning remote alerts.

| Event                          | Action                                                                                                                                                                                                                                                                                          | Numeric code |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| Single fan failure             | Generates an alert if one fan fails.                                                                                                                                                                                                                                                            | 11           |
| Temperature irregularity       | Generates an alert if any monitored temperatures are outside the warning threshold values. These temperature threshold values are accessed by clicking the temperature readings on the System Health page. Unlike the critical temperature event, this event will not initiate system shutdown. | 12           |
| Voltage irregularity           | Generates an alert if any monitored voltages are outside the warning threshold values. These voltage range values are accessed by clicking the voltage readings on the System Health page. Unlike the critical voltage event, this event will not initiate an automatic system shutdown.        | 13           |
| Redundant power supply failure | Generates an alert if a redundant power supply fails.                                                                                                                                                                                                                                           | 10           |

### System alerts

System alerts are generated for events that occur as a result of system errors. The **Select all system alerts** check box enables you to have an alert sent for any system alert.

**Notes:**

- a. The Select all system alerts check box is not available on all systems.
- b. Hard disk drive Predictive Failure Analysis® (PFA) alerts are not monitored.

Table 10. System remote alerts.

| Event            | Action                                                                                                                                                                                                                                            | Numeric code |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| Boot failure     | Generates an alert if an error occurs that prevents the system from starting.                                                                                                                                                                     | 25           |
| Loader timeout   | Generates an alert if an enabled system loader timeout value is exceeded. The system loader timeout value is configured in the Server Timeouts section on the System page.                                                                        | 26           |
| 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. This alert must be checked to enable remote blue screen capture. | 21           |
| PFA notification | Generates an alert if a PFA notification is generated by the system hardware. This feature is available only on systems that have PFA-enabled hardware.                                                                                           | 27           |
| 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.                                                                                          | 20           |
| Power off        | Generates an alert if the system is turned off.                                                                                                                                                                                                   | 23           |
| Power on         | Generates an alert if the system is turned on.                                                                                                                                                                                                    | 24           |

- 4. Click **Save**.

Continue with “Setting local events”.

## Setting local events

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

- 1. Log into the Remote Supervisor Adapter where you want to set local events. For more information, see Chapter 2, “Opening and using the ASM Web interface,” on page 3.
- 2. In the navigation frame, 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 stores the notification only in the event log.

In a future release of the IBM Director, local events will be sent to the server where the Remote Supervisor Adapter resides. These events will not be sent to remote alert recipients. The **Select all local events** check box enables you to have an alert sent for any local event.

Table 11. 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 powered 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 only available 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 system generates a PFA.                              |

4. Click **Save**.

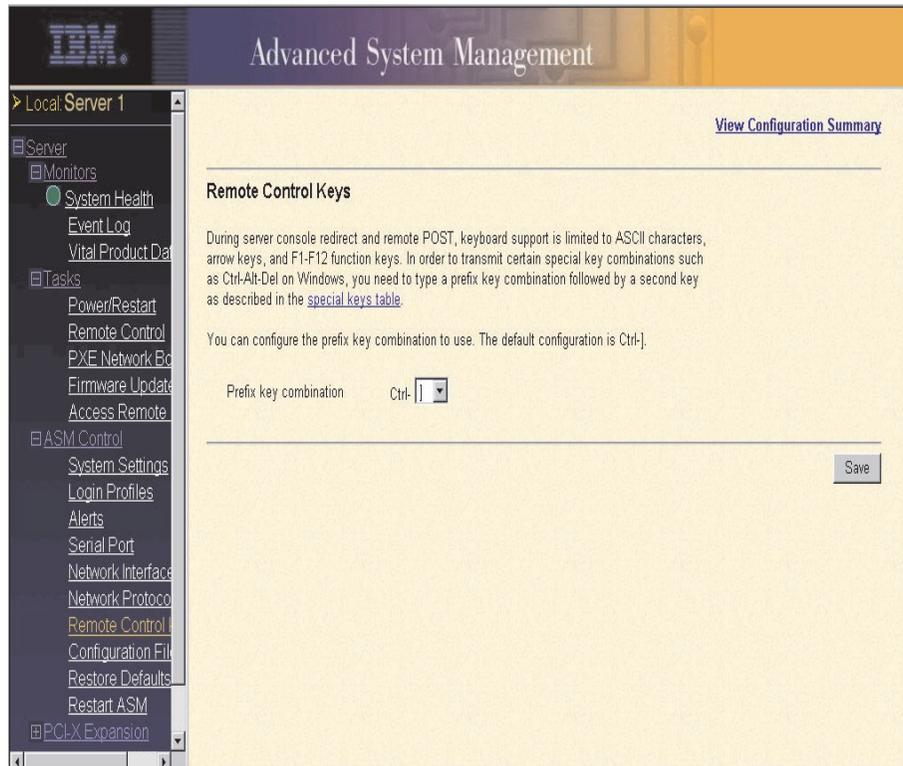
---

## Configuring remote control keys

During server console redirect and remote POST, keyboard support is limited to ASCII characters, the arrow keys, and the F1 through F12 function keys. To transmit certain special key combinations, such as Ctrl+Alt+Del on Microsoft Windows operating systems, you must type a prefix key combination followed by a second key as described in the special keys table. You can define the prefix key combination that you want to use, as shown in the following illustration. The default prefix key combination is Ctrl+]. To view the special keys table, click **special keys table** in the Remote Control Keys window.

Complete the following steps to configure prefix key combinations.

1. Log into the Remote Supervisor Adapter where you want to configure the prefix key combination. For more information, see Chapter 2, “Opening and using the ASM Web interface,” on page 3.
2. In the navigation frame, click **Remote Control Keys**. A window similar to the following opens:



3. Follow the directions in the window to select the desired prefix key combination.
4. Click **Save**.

---

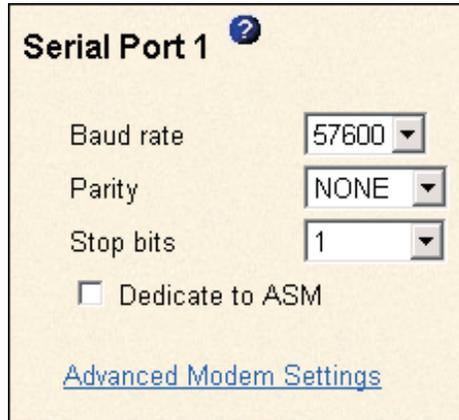
## Configuring the serial port

You can either dedicate the integrated serial port on the Remote Supervisor Adapter to system management or share it with the server operating system. If dedicated to system management, the serial port serves only the Remote Supervisor Adapter and is always available for dial-in and dial-out alerting purposes. You will not be able to monitor the port on the network operating system (NOS) or in any other applications.

This design enables a single serial port to conduct normal functions and also maintain out-of-band alerting capabilities.

Complete the following steps to configure your serial port. For more information on your serial port, see “Configuring PPP access over a serial port” on page 45.

1. Log into the Remote Supervisor Adapter where you want to configure the serial port. For more information, see Chapter 2, “Opening and using the ASM Web interface,” on page 3.
2. In the navigation frame, click **Serial Port**. A window similar to the following opens:



**Serial Port 1** ?

Baud rate: 57600

Parity: NONE

Stop bits: 1

Dedicate to ASM

[Advanced Modem Settings](#)

3. In the Baud rate field, select the data transfer rate.  
Use the Baud rate field to specify the data transfer rate of your serial port connection. To set the baud rate, select the data transfer rate in bits per second that corresponds to your serial port connection.
4. In the Parity field, select the error detection to be used in your serial connection.  
Use the Parity field to specify the error detection bit 0 or 1 added to each group of transmitted bits so that it will have either an odd or even number of 1s. This enables your server to know whether received data has been corrupted during transmission.
5. Select the number of data-terminating 1-bits in the Stop bits field that will follow the data or any parity bit to mark the end of a transmission (normally a byte or character).  
**Note:** The number of data bits is preset to 8 and cannot be changed.
6. Click the **Dedicate to ASM** check box to reserve the serial port for the Remote Supervisor Adapter.  
When shared with the operating system, the serial port serves the Remote Supervisor Adapter only while the server is turned off or during the power-on self-test (POST). The operating system can access it after the POST completes. Only after a critical event will the Remote Supervisor Adapter take over the port from the NOS to dial-out and transmit an alert. The port then remains under Remote Supervisor Adapter control until the server is restarted.  
**Note:** If you have configured a PPP interface, dedicate the serial port to the Remote Supervisor Adapter or you will lose the PPP port when the host restarts.
7. Click **Save**.

8. If you need to set advanced settings, click **Advanced Modem Settings**. A window similar to the following opens:

### Port 1 Modem Settings 2

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

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

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

Set these values only if the alert forwarding functions are not working properly. The strings marked with an asterisk (\*) require a carriage return (^M) to be manually entered at the end of the field value.

The following table describes the initialization strings for this modem.

Table 12. 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 if the modem is attached. The default is AT.                                                                                                          |

Table 12. Port 1 settings.

| Field                   | What you type                                                                                                                                                         |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Factory settings string | Type the initialization string that returns the modem to its factory settings when the modem is initialized. The default is AT&F0.                                    |
| Auto answer             | Type the initialization string that is used to tell the modem to answer the phone when it rings. The default is to answer after one ring or ATSO=1.                   |
| Escape string           | Type the initialization string that returns the modem to command mode when it is currently talking to another modem. The default is +++.                              |
| Auto answer stop        | Type the initialization string that is used to tell the modem to stop answering the phone automatically when it rings. The default is ATSO=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 time before and after the escape string is issued to the modem. This value is measured in 10 millisecond intervals. The default value is 1 second. |

9. Click **Save**.

## Initialization-string guidelines

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

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

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

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

---

## Configuring an Ethernet connection to ASM

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

1. Log into the Remote Supervisor Adapter where you want to restore the configuration. For more information, see Chapter 2, “Opening and using the ASM Web interface,” on page 3.
2. In the navigation frame, click **Network Interfaces**.

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

The screenshot shows a configuration window titled "Ethernet" with a help icon. It contains the following fields and options:

- Interface: A dropdown menu set to "Enabled".
- DHCP: A dropdown menu set to "Disabled - Use static IP configuration".
- Hostname: A text input field containing "testsite".
- Static IP Configuration section with three text input fields:
  - IP address: "9.67.41.96"
  - Subnet mask: "255.255.255.0"
  - Gateway address: "9.67.41.1"

At the bottom, there are two links: "IP Configuration Assigned by DHCP Server" and "Advanced Ethernet Setup".

3. If you want to use an Ethernet connection, in the Interface field, select **Enabled**. It is enabled by default.
4. If you want to use a dynamic host configuration protocol (DHCP) server connection, enable the DHCP field. It is enabled by default. Go to step 12.

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

If DHCP is enabled, the Hostname field is used as follows:

- If the Hostname field is set, then the Remote Supervisor Adapter DHCP support will request the DHCP server to allow the use of this host name.
  - If the Hostname field is not set, then the Remote Supervisor Adapter DHCP support will request the DHCP server to assign a unique host name to the Remote Supervisor Adapter.
5. In the Hostname field, type the IP host name of the Remote Supervisor Adapter.

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

**Note:** The IP host name of the Remote Supervisor Adapter (the Hostname field) and Remote Supervisor Adapter 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 while the Host Name field can consist of up to 63 characters. To minimize confusion, set the ASM Name field to the non-qualified portion of the IP host name. The non-qualified IP host name consists of up to the first period of a fully qualified IP host name. For example, the non-qualified IP host name of `asmcard1.us.company.com` (a fully qualified IP host name) is `asmcard1`. For more information on your host name, see "Setting system information" on page 26.

6. In the IP address field, type the IP address of the Remote Supervisor Adapter. You must do this only if DHCP is disabled. The IP address must contain:
  - Four integers from 0 to 255 separated by periods
  - No spaces

7. In the Subnet mask field, type the subnet mask used by the Remote Supervisor Adapter. You must do this only if DHCP is disabled. The subnet mask must contain:
  - Four integers from 0 to 255 separated by periods
  - No spaces or consecutive periods
 The default setting is 255.255.255.0.
8. In the Gateway address field, type your network gateway router. You must do this only if DHCP is disabled. The gateway address must contain:
  - Four integers from 0 to 255 separated by periods
  - No spaces or consecutive periods
9. Click the **Save** button.
10. Click **Advanced Ethernet Setup** if you need to set additional Ethernet settings.

### Advanced Ethernet Setup ?

Data rate Auto ▾

Duplex Auto ▾

Maximum transmission unit 1500 bytes

Locally administered MAC address 00:00:00:00:00:00

Burned-in MAC address: 00:02:55:38:07:56

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

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

Table 13. Advanced Ethernet setup.

| Field     | Function                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data rate | <p>Use the Data Rate field to specify the amount of data to be transferred per second over your LAN connection.</p> <p>To set the data rate, click the menu and select the data transfer rate in megabits (Mb) that corresponds to the capability of your network. To automatically detect the data transfer rate, select Auto, which is the default value.</p>                                                                                  |
| Duplex    | <p>Use the Duplex field to specify the type of communication channel used in your network.</p> <p>To set the duplex mode, select one of the following:</p> <p><b>Full</b> Enables data to be carried in both directions at once.</p> <p><b>Half</b> Enables data to be carried in either one direction or the other, but not both at the same time.</p> <p>To automatically detect the duplex type, select Auto, which is the default value.</p> |

Table 13. Advanced Ethernet setup.

| Field                            | Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maximum transmission unit        | Use this 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 by the manufacturer. The address is also a read only field.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Locally administered MAC address | Enter a physical address for this Remote Supervisor Adapter 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 between 000000000000 - FFFFFFFF. This value must be in the form XX:XX:XX:XX:XX:XX where X is a number between 0 and 9. The Remote Supervisor Adapter does not support the use of a multicast address. A multicast address has the least significant bit of the first byte set to 1. The first byte, therefore, must be an even number. |

11. Modify the advanced Ethernet settings as necessary.
12. 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.  
  
In order to view the DHCP server assigned setting, click **IP Configuration Assigned by the DHCP Server**.
15. Click **Save**.
16. In the navigation frame, click **Restart ASM** to activate the changes.

## Configuring PPP access over a serial port

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 through a TELNET session or a Web browser.

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

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

1. Log into 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 ASM Web interface," on page 3.
2. In the navigation frame, click **Network Interfaces**. Scroll down to the PPP over Serial Port section.

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

**PPP over Serial Port** ?

|                   |                 |
|-------------------|-----------------|
| Interface         | Disabled ▾      |
| Local IP address  | 192.96.1.1      |
| Remote IP address | 192.96.1.2      |
| Subnet mask       | 255.255.255.255 |
| Authentication    | CHAP then PAP ▾ |

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. The field defaults to 192.96.1.1. The IP address must contain:
  - Four integers from 0 to 255 separated by periods
  - No spaces
5. In the Remote IP address field, type the remote IP address that this Remote Supervisor Adapter will assign to a remote user. The field defaults to 192.96.1.2. The remote IP address must contain:
  - Four integers from 0 to 255 separated by periods
  - No spaces
6. In the Subnet mask field, type the subnet mask for the Remote Supervisor Adapter to use. The default is 255.255.255.255. The subnet mask must contain:
  - Four integers from 0 to 255 separated by periods
  - No spaces
7. 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. This weak 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. This is a stronger authentication protocol than the PAP Only setting 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 will be tried as a secondary authentication protocol. The **CHAP then PAP** setting is the default.
8. Click **Save**.
9. In the navigation frame, click **Restart ASM** to activate the changes.

## Configuring SNMP

The simple network management protocol (SNMP) enables you to 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 are planning to configure SNMP trap alerts on the Remote Supervisor Adapter, you must install and compile the supplied management information base (MIB) on your SNMP manager. For more information on the MIB file, see your *Remote Supervisor Adapter Installation Guide*.

Complete the following steps to configure your SNMP:

1. Log into the Remote Supervisor Adapter where you want to configure SNMP. For more information, see Chapter 2, “Opening and using the ASM Web interface,” on page 3.
2. Specify a system contact and the system location information on the **System** page. For more information on the System page settings, see “Setting system information” on page 26.
3. In the navigation frame, click **Network Protocols**. A window similar to the following opens:

**Simple Network Management Protocol (SNMP)**

SNMP agent

SNMP traps

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

4. Enable the SNMP agent and SNMP traps fields.

Enabling the SNMP agent field forwards 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 page. For more information on the System page settings, see “Setting system information” on page 26.
- System location must be specified on the System 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 SNMP traps and the SNMP agent are enabled.

- 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, you will not be granted SNMP management access.

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

- In the Community Name field, enter a name or authentication string that corresponds to the desired community.
- In the corresponding Host Name or IP Address field, enter the host name or IP addresses of each community manager.
- Scroll to the Domain Name System (DNS) section. A window similar to the following opens:

### Domain Name System (DNS) ?

DNS Enabled ▾

DNS server IP address 1 9.37.0.5

DNS server IP address 2 9.37.0.6

DNS server IP address 3 0.0.0.0

**Host Table (IP Address to Host Name Mappings)**

|    | IP Address | Host Name |
|----|------------|-----------|
| 1. | 0.0.0.0    |           |
| 2. | 0.0.0.0    |           |
| 3. | 0.0.0.0    |           |
| 4. | 0.0.0.0    |           |

- If a DNS server (or servers) is available on your network, enable the DNS option in the DNS field.

The DNS field specifies whether you use a DNS server on your network to translate host names into IP addresses.

- If you enabled DNS in the DNS server IP address fields, enter the IP address of up to three DNS servers.

The DNS fields specify the IP addresses of up to three DNS servers on your network. Each IP address should contain integers from 0 to 255, separated by periods.

**Notes:**

- Enter an IP address in the IP Address field and its corresponding host name in the Host Name field. You can define four mappings. You only need to do this if a quick lookup of a host name is required.

Use the fields in the Host Name section to define relationships between an IP address and its corresponding host name in the event that your network DNS server is unreachable. You can also use these mappings for frequently used host names.

- b. The Remote Supervisor Adapter uses this table when first searching for an address to host name mapping. If a match is not found, the data will be requested from the DNS server. If the table contains an entry for a given address, the host name defined in the table will override any corresponding entry defined on the DNS server.
11. Click **Save**.
  12. In the navigation frame, click the **Restart ASM** link 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:

1. Log into the Remote Supervisor Adapter where you want to configure the SMTP. For more information, see Chapter 2, “Opening and using the ASM Web interface,” on page 3.
2. In the navigation frame, 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.

---

## Backing up your current configuration

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

Complete the following steps to back up your current configuration:

1. Log into the Remote Supervisor Adapter where you want to backup your current configuration. For more information, see Chapter 2, “Opening and using the ASM Web interface,” on page 3.
2. In the navigation frame, 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 and choose the location where the file will be saved, then click **Save**.

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

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

## Restoring your ASM configuration

You can restore a saved configuration in full. Complete the following steps to restore your current configuration:

1. Log into the Remote Supervisor Adapter where you want to restore the configuration. For more information, see Chapter 2, “Opening and using the ASM Web interface,” on page 3.
2. In the navigation frame, click **Configuration File**.
3. In the Restore ASM Configuration section, click **Browse**.
4. Click the configuration file that you want and then click **Open**. The file (including the full path) appears in the box beside **Browse**.
5. If you want to change the configuration file before restoring, click **Modify and Restore**. Otherwise, click **Restore**.

A new page opens with the ASM configuration in it. If you selected **Modify and Restore**, you can make changes to certain fields on this page.

6. Verify that this is the configuration that you want to restore. If it is not the correct file, click **Cancel**.
7. To proceed with restoring this file to the Remote Supervisor Adapter, click **Restore Configuration**.
8. After receiving a confirmation that the restore process is complete, go to the Restart ASM page and click **Restart**.
9. Click **OK** to confirm that you want to restart your Remote Supervisor Adapter.
10. Click **OK** to close the current browser window.
11. To log into the Remote Supervisor Adapter again, open your browser and follow your regular login process.

## Restoring a changed configuration

You can modify key fields in the saved configuration before restoring them to your Remote Supervisor Adapter. Modifying the configuration before restoring helps you to set up multiple Remote Supervisor Adapters 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 a changed configuration:

1. Log into the Remote Supervisor Adapter that has the configuration that you want to restore. For more information, see Chapter 2, “Opening and using the ASM Web interface,” on page 3.
2. In the navigation frame, click **Firmware Update**.
3. Click **Browse** in the Restore ASM Configuration section.
4. Navigate to the configuration file and then click **Open**. The file (including the full path) appears in the box beside **Browse**.
5. Click **Modify and Restore** to open an editable configuration summary page. 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 page.
6. To modify the contents of any field, click in the corresponding text box and enter the data.
7. Verify that the displayed configuration is what you want to restore.

8. Click **Restore Configuration**. A progress indicator appears as the firmware on the Remote Supervisor Adapter is flashed. A confirmation page appears to verify whether the update was successful.
9. After receiving a confirmation that the restore process is complete, go to the Restart ASM page. In the navigation frame, click **Restart**.
10. Click **OK** to confirm that you want to restart your ASM Web interface.
11. Click **OK** to close the current browser window.
12. To log into the Remote Supervisor Adapter again, open your browser and follow your regular login process.

---

## Restoring ASM defaults

This link enables you to restore the default configuration of the Remote Supervisor Adapter 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. You also lose the remote control of the remote servers. You will have to reset the password locally on the remote servers during BIOS code setup if you click Restore Defaults.

1. Log into the Remote Supervisor Adapter. For more information, see Chapter 2, “Opening and using the ASM Web interface,” on page 3.
2. In the navigation frame, click **Restore Defaults** to restore default settings of the Remote Supervisor Adapter. You will lose your TCP/IP connection.
3. Login again to use the ASM Web interface.
4. Reconfigure the network interface to restore connectivity. For more information on the network interface, see “Configuring an Ethernet connection to ASM” on page 42.

---

## Restarting ASM

The following links enable you to restart the Remote Supervisor Adapter if you have read/write access.

1. In the navigation frame, click **Restart ASM** to restart the Remote Supervisor Adapter. Your TCP/IP or modem connections are broken.
2. Login again to use the ASM Web interface.

---

## Logging off

Complete the following steps to log off of the Remote Supervisor Adapter:

1. In the navigation frame, click **Log Off**.
2. If you are running Internet Explorer or Netscape Navigator, click **Yes** in the confirmation window.

This closes the current browser window and thereby maintains security. You must manually close other open browser windows, if any, or a cached version of your user ID and password remain available.



## Chapter 6. Starting and configuring the ASM text-based interface

You can access the Remote Supervisor Adapter through the text-based user interface in the Advanced System Management window by establishing a TELNET connection or a direct serial connection.

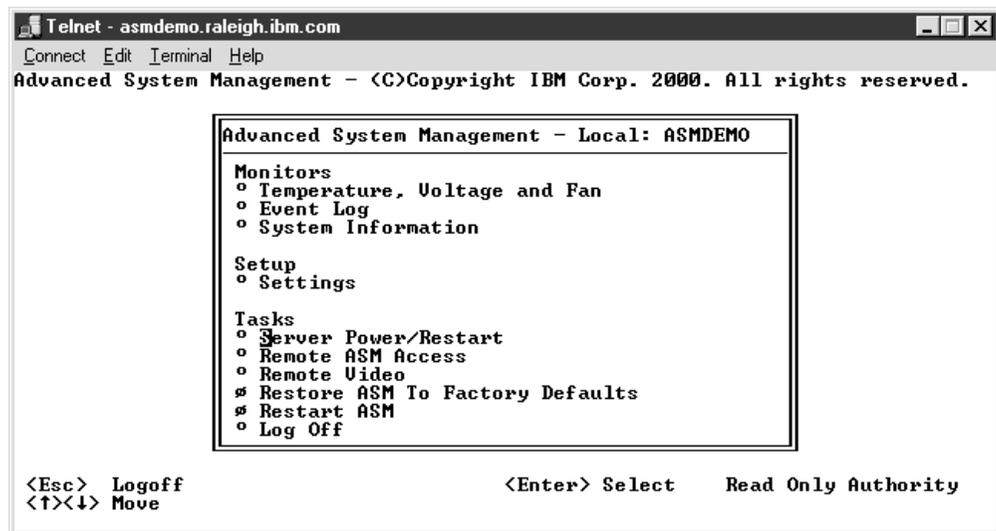
**Note:** F1 through F4 are the only function keys that are supported in the text-based interface.

### Accessing a text-based interface via a TELNET connection

Complete the following procedure to access the Remote Supervisor Adapter through a TELNET connection:

1. Open a command prompt.
2. Type TELNET and either the host name or IP address at the command prompt.  
A TELNET client opens.
3. Configure the TELNET client for the text-based user interface. For more information on configuring a text-based user interface, see “Configuring terminal settings” on page 54.
4. Type a user name in the Login ID field.
5. Type the password associated with the user name in the Password field. The Advanced System Management window opens.

**Note:** This screen is an example of a TELNET client. Your settings might be different.



```
Telnet - asmdemo.raleigh.ibm.com
Connect Edit Terminal Help
Advanced System Management - (C)Copyright IBM Corp. 2000. All rights reserved.

Advanced System Management - Local: ASMDEMO

Monitors
  o Temperature, Voltage and Fan
  o Event Log
  o System Information

Setup
  o Settings

Tasks
  o Server Power/Restart
  o Remote ASM Access
  o Remote Video
  o Restore ASM To Factory Defaults
  o Restart ASM
  o Log Off

<Esc> Logoff          <Enter> Select      Read Only Authority
<↑><↓> Move
```

**Note:** Press the Up Arrow and Down Arrow keys to navigate this screen. Press Esc to exit to the Advanced System Management window; if you press Esc at the Advanced System Management window, you log off of your session. Press F3 to exit the window you are viewing.

---

## Accessing a text-based interface via a direct serial connection

Complete the following procedure to set a direct serial connection:

1. Connect a null modem cable to the serial port of the Remote Supervisor Adapter.
2. Connect the other end of the cable to a COM port on the client computer.
3. Start a terminal emulation program on the client computer such as Hilgraeve HyperTerminal.
4. Select the **File** → **Properties** menu option. The New Connection Properties window opens.
5. Click **Configure** and set the following values:

Table 14. COM properties.

| Field           | Entry |
|-----------------|-------|
| Bits per second | 57600 |
| Data bits       | 8     |
| Parity          | None  |
| Stop bits       | 1     |
| Flow control    | None  |

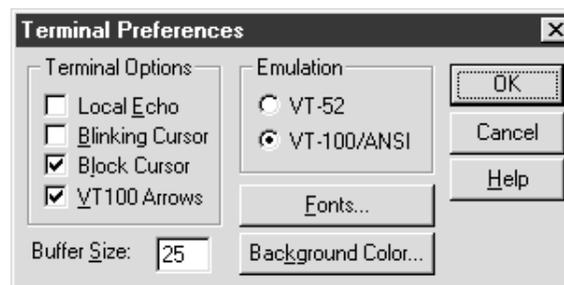
6. Click **OK**.
7. Click the **Settings** tab.
8. From the Emulation field, select **Terminal Keys** and **ANSI**.
9. Click **OK**.
10. Select **View** → **Font**.
11. Select the Terminal font with a point size of 9.
12. Click **OK**.
13. Press Esc to begin your session. The login prompt opens.
14. Enter your login ID and password.

---

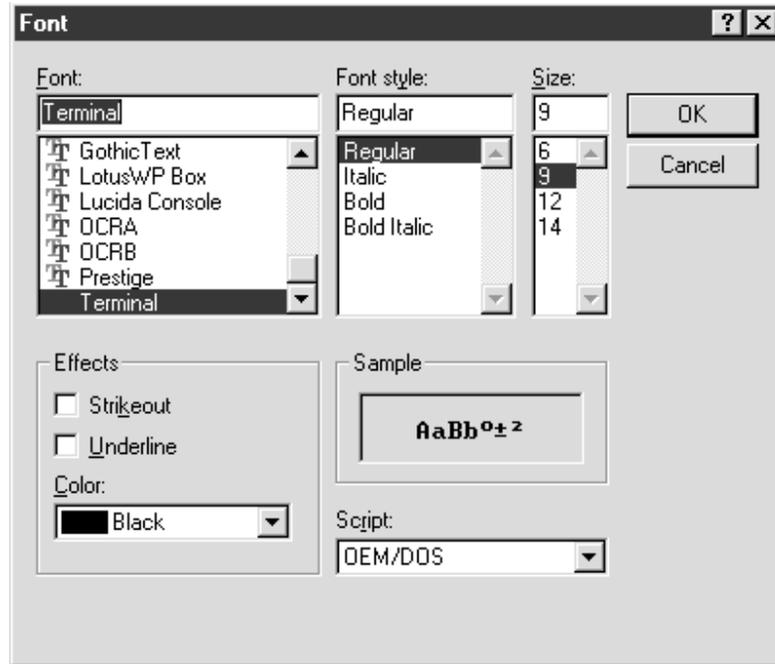
## Configuring terminal settings

Complete the following procedure to properly display special characters in the text-based user interface:

1. Select **Terminal** → **Preferences**. The Terminal Preferences window opens.



2. Select the following check box options:
  - **Blinking Cursor** or **Block Cursor**
  - **VT100 Arrows**
  - **VT-100/ANSI**
3. Click **Fonts**. The Font window opens.



4. From the Font window, select the Terminal font. In the Size window, select 9 for the font size.
5. Click **OK**.



---

## Chapter 7. Configuring your Remote Supervisor Adapter using a text-based interface

In the Advanced System Management window, use the Settings options under the ASM Setup heading to configure your Remote Supervisor Adapter values.

**Note:** F1 through F4 are the only function keys that are supported in the text-based interface.

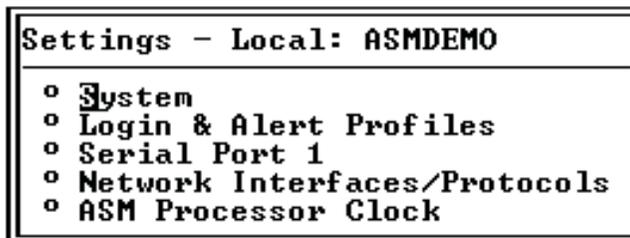
- From the System window, you can:
  - Set system information
  - Set server timeouts, which will result in automatic corrective action by the Remote Supervisor Adapter
- From the Login & Alert Profiles window, you can:
  - Set login profiles to control access to the Remote Supervisor Adapter
  - Configure modem/dial-in settings
  - Configure remote alert recipients
  - Set the number of remote alert attempts
  - Select alerts that will be monitored/sent
  - Select local events to track
  - Set e-mails to include the event log attachment when alerts are generated
- From the Serial Port 1 window, you can:
  - Configure the serial port to the Remote Supervisor Adapter
  - Configure advanced modem settings
- From the Network Interfaces/Protocols window, you can:
  - Set up an Ethernet connection to the Remote Supervisor Adapter
  - Set up a PPP over serial port connection to the Remote Supervisor Adapter
  - Configure SNMP setup
  - Configure DNS setup
  - Configure SMTP setup
- From the ASM Processor Clock window, you can set the ASM date and time.

---

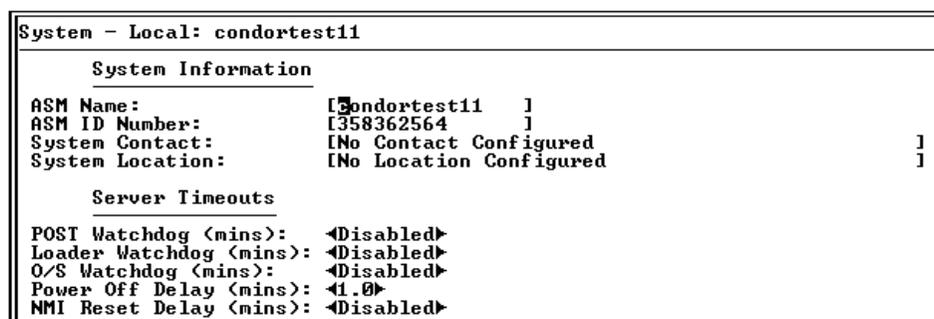
### Setting system information

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

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 53.
2. In the Advanced System Management window, select **Settings**. The Settings window opens:



3. In the Settings window, select **System**. A window similar to the following opens:



4. In the ASM Name field, type the name of the Remote Supervisor Adapter.

Use the ASM Name field to specify a name for the ASM in this server. This name is included in e-mail, SNMP, and alphanumeric pager alert notifications to identify the source of the alert.

**Note:** Your Remote Supervisor Adapter name (the ASM Name field) and IP host name of the Remote Supervisor Adapter (the Host name field on the Network Interfaces window) do not automatically share the same name because the ASM Name field is limited to 15 characters. The Host name field can consist of up to 63 characters. To minimize confusion, set the ASM Name field to the non-qualified portion of the IP host name. The non-qualified IP host name consists of up to the first period of a fully qualified IP hostname. For example, the non-qualified IP host name of `asmcard1.us.company.com` (a fully qualified IP host name) is `asmcard1`. For more information on your host name, see “Configuring an Ethernet connection to ASM” on page 72.

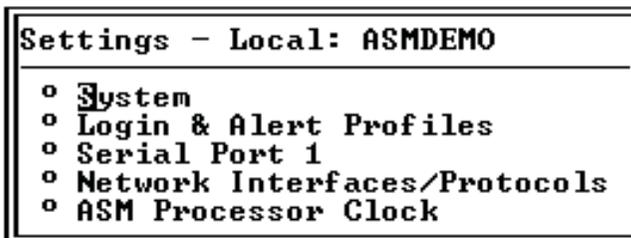
5. In the System Contact field, type contact information. For example, you can specify the name and phone number of the person to contact if there is a problem with this server. You can type a maximum of 47 characters in this field.
6. In the System Location field, type the location of the server. Include 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.

---

## Setting server timeouts

Complete the following steps to set your server timeout values:

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 53.
2. In the Advanced System Management window, select **Settings**. The Settings window opens:



3. In the Settings window, select **System**.
4. In the system window, use the Down Arrow key to move to the Server Timeouts section. You can set the Remote Supervisor Adapter to automatically respond 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
5. Enable the server timeouts that correspond to the events you want the Remote Supervisor Adapter to respond to automatically.

#### **POST Watchdog**

Use the POST Watchdog <mins> field to specify the number of minutes that the Remote Supervisor Adapter will wait for this 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 generates a POST time-out 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 if the operating system and device driver successfully loads).

**Note:** Power-cycling differs from shutting down and restarting the operating system in that power-cycling removes power from the server completely. For example, unplugging your server.

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

**Note:** If the **POST timeout** option is selected in the System Remote Alerts window, the Remote Supervisor Adapter attempts to forward the alert to all enabled 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 will be ignored.

Refer to your server documentation for further details.

#### **Loader Watchdog**

Use the Loader Watchdog <mins> field to specify the number of minutes that the Remote Supervisor Adapter waits between the completion of POST and the loading of the operating system. If this interval is exceeded, the Remote Supervisor Adapter generates a loader time-out alert and automatically restarts the system. After the system is restarted, the loader time-out is automatically disabled until the operating system is shut down and the server is power-cycled (or the operating system and device driver successfully load).

To set the loader time-out value, select the time limit that the Remote Supervisor Adapter will wait for operating-system loading to complete. To turn off this option, select **Disabled**.

**Note:** If the **Loader Timeout** option is selected in the System Remote Alerts window, the Remote Supervisor Adapter will send an alert to all enabled remote alert recipients.

### O/S Watchdog

Use the O/S Watchdog <mins> field to specify the number of minutes between checks of the operating system by the Remote Supervisor Adapter. If the operating system fails to respond to one of these checks, the Remote Supervisor Adapter generates an operating system time-out alert and automatically restarts the server. After the server is restarted, the operating system is power-cycled.

To set the operating-system watchdog value, select a time interval from the menu. To turn off this option, select **Disabled**. To capture blue screens, you must enable the O/S Watchdog field and make sure that the **O/S Timeout** option is disabled until the operating system is shut down and the server completes a power-cycle.

#### Notes:

- a. The operating-system watchdog feature requires that the IBM System Management device driver be installed on the server.
- b. If the O/S Timeout option is selected in the System Remote Alerts window, the Remote Supervisor Adapter will attempt to send an alert to all enabled remote alert recipients.

### Power Off Delay

Use the Power Off Delay field to specify the number of minutes that the Remote Supervisor Adapter will wait for the operating system to shut down before turning off the server. By default, the Remote Supervisor Adapter waits 30 seconds.

Shut down your server to determine how long it takes to shutdown. Add a time buffer to that value and use it as your power-off delay setting.

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

**Attention:** You must have the UM Server Extensions agent code installed to enable an orderly operating system shutdown. Even with this code installed, you could lose or corrupt data on your server. For more information on installing UM server extension code for the Remote Supervisor Adapter, see your *UM Server Extensions User's Guide*. For the operating system to receive the shutdown notification from the Remote Supervisor Adapter, the server must have the ASM device driver and the ASM component of UM Server Extensions installed.

### NMI reset delay

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

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

To set the NMI reset delay value, click the pull-down button and select the desired number of minutes. To disable the automatic server restart after a non-maskable interrupt, select **Disabled**.

---

## Creating a login profile

Complete the following steps to configure a login profile:

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 53.
2. In the Advanced System Management window, select **Settings**. The Settings window opens:

```
Settings - Local: ASMDEMO
├─ System
├─ Login & Alert Profiles
├─ Serial Port 1
├─ Network Interfaces/Protocols
└─ ASM Processor Clock
```

3. In the Settings window, select **Login & Alert Profiles**. The Login and Alerts Profiles window opens:

```
Login & Alert Profiles - Local: ASMDEMO
├─ Login Configuration
│  └─ Login Settings
│  └─ Login Profiles
├─ Alert Configuration
│  └─ Remote Alert Settings
│  └─ Remote Alert Recipients
│  └─ Critical/Warning Remote Alerts
│  └─ System Remote Alerts
│  └─ Events For Local Notification
```

4. In the Login and Alert Profiles section, select **Login Profiles**.

```
Log Login Profiles - Local: ASMDEMO
├─ Administrator
├─ guest1
├─ guest2
├─ guest3
├─ guest4
├─ guest5
├─ guest6
├─ guest7
├─ guest8
├─ guest9
├─ guest10
└─ dp
```

Use the Login Profiles window to view, configure, or change individual login profiles. You can define up to twelve unique profiles. If you have not configured a

profile, the name of the profile by default will be User *nn* where *nn* is an arbitrary number assigned to that profile.

To work with a login profile, select a profile name. A window similar to the following opens:

```

User 2 - Local: ASMDEMO
-----
Login Profile
Login ID:      [guest1      ]
Password:     [              ]
Confirm Password: [          ]
Authority Level: <Read Only>

Dial Back Settings
Status:       <Disabled>
Number:      [              ]
# Reset Entry To Defaults
  
```

5. In the Login ID field, type the name of the profile.  
 You can type a maximum of fifteen 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.
6. In the Password field, assign a password for the login ID.  
 To set the password, type the password in both the Password and Confirm Password fields.  
 Valid passwords must contain at least five characters, one of which must be a non alphabetic 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.
7. In the Authority Level field, select either **Read Only** or **Read/Write**.  
 Use the Authority Level field to set the access rights for this login ID.  
**Read-Only**  
 Enables the user to view a page but not to make changes. Additionally, people who log in with read-only IDs are unable to perform file transfers, power and restart actions, or remote control functions.  
**Read/Write**  
 Enables the user to take all available actions provided by the interface, including setting up a user ID and turning off the server.
8. Select **Enabled** in the Status field of the Dialback Settings option to configure the Remote Supervisor Adapter to automatically terminate a successful dial-in attempt, and then immediately dial-out to a specified number. Otherwise, go to step 10 on page 63.  
**Note:** If this menu is enabled, you must enter a phone number in the Number field of this profile.
9. In the Number field, type the phone number the Remote Supervisor Adapter will use when dialing back.  
 This phone number is dialed when the user profile successfully logs into the Remote Supervisor Adapter.  
**Note:** By default, the Remote Supervisor Adapter is configured with one login profile that enables remote access using a login user ID of USERID and a

password of PASSWORD (the 0 is a zero). To avoid a potential security exposure, change this default login profile during initial setup of the Remote Supervisor Adapter.

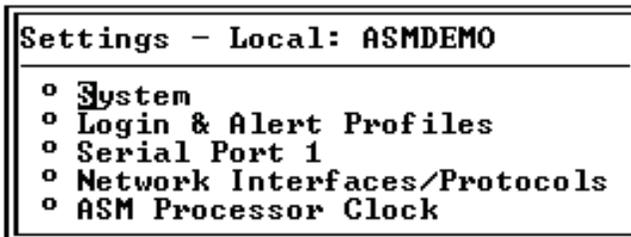
10. If you want a remote user to dial into the Remote Supervisor Adapter through a connection, press F3 twice to return to the Login & Alert Profiles window.

---

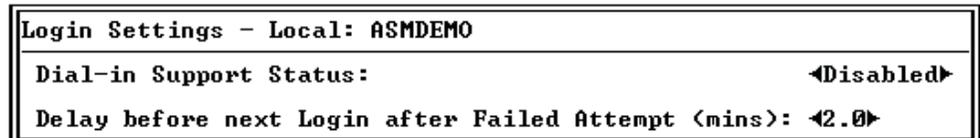
## Setting modem and dial-in settings

Complete the following steps to enable your modem to dial out to the remote login profile:

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 53.
2. In the Advanced System Management window, select **Settings**. The Settings window opens:



3. Select **Login & Alert Profiles**.
4. In the Login and Alert Profiles window, select **Login Settings**.



5. In the Dial-in Support Status field, select **Enabled** to enable remote users to dial into the Remote Supervisor Adapter through a serial connection.
6. Use the Delay before next Login after Failed Attempt <mins> field to specify how long, in minutes, the Remote Supervisor Adapter will prohibit remote login attempts when more than five sequential remote login failures are detected.

---

## Configuring remote alert recipients

You can configure the remote alert recipients, number of alert attempts, incidents that trigger remote alerts, and local alerts. Use these remote alert recipient links to view, configure, or change individual alert recipients. You can define up to twelve unique recipients. Each link for an alert recipient is labeled with the recipient name.

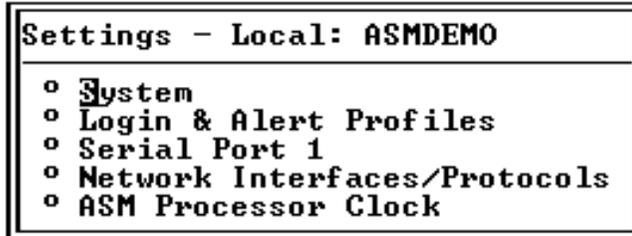
When you configure a remote alert entry, the Remote Supervisor Adapter, ASM processor, or ASM PCI adapter sends an alert to a remote system (through a serial connection or a network connection), a numeric pager, or an alphanumeric pager when an event selected from the Enabled Alerts group occurs. This alert will contain information about the nature of the event, the time and date of the event, and the name of the system that generated the alert.

If the SNMP Agent or SNMP Traps fields are not enabled, no SNMP type alerts will be sent. For more information on these fields, see “Configuring SNMP” on page 77.

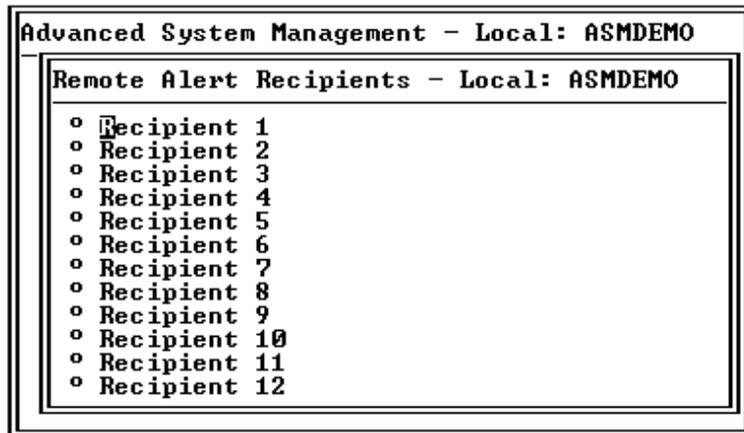
**Note:** You cannot distinguish between what alerts will be sent to which remote alert recipient. All configured recipients receive each alert you select.

Complete the following steps to configure a remote alert recipient:

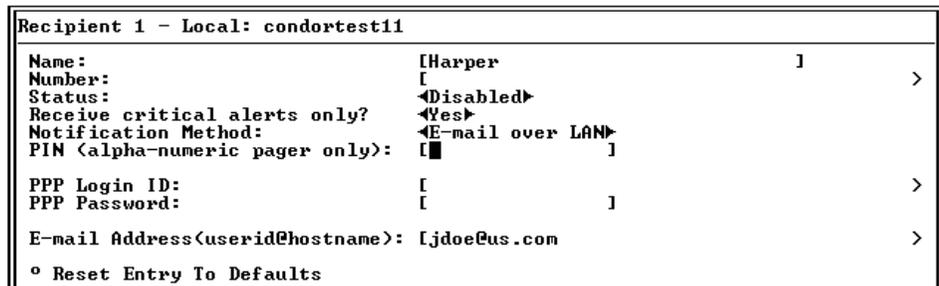
1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 53.
2. In the Advanced System Management window, select **Settings**. The Settings window opens:



3. In the Login and Alert Profiles window, select **Remote Alert Recipients**.



4. Select a remote alert recipient option. An individual recipient page similar to the following appears.



5. In the Name field, type the name of the recipient or the transmission method. The name that you enter appears as the recipient name on the Remote Alert Recipients window.

6. In the Number field, type either the phone number, IP address, or host name for 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 a personal identification number [PIN])
- Alphanumeric pager
- IBM Director over modem
- SNMP over PPP
- E-mail over PPP

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

7. In the Status field, select **Enabled**. This field enables you to activate or deactivate remote alert recipients.
8. Select **Enabled** in the Receive critical alerts only field if the recipient should only receive critical alerts.
9. Select the notification method for reaching the recipient in the Notification Method field. Select from one of the following notification methods:

- Numeric pager
- Alphanumeric pager
- IBM Director over Modem
- IBM Director over LAN
- SNMP over LAN
- E-mail over LAN
- SNMP over PPP
- E-mail over PPP

**Note:** If you select to send remote alerts by the IBM Director over Modem or IBM Director over LAN options, you must have the ASM component of UM Server Extensions installed on the IBM Director Server.

10. If you chose alphanumeric pager as the notification method, enter the PIN in the PIN (alpha-numeric pager only) field.
11. If you select the E-mail over PPP or SNMP over PPP notification methods, type the login ID needed to log into the recipient's dial-up service account at the PPP Login ID field. The PPP login ID consists of a secure IP address, an account name, and a user ID all separated by periods.

For example, to log into the IBM Global Network IP Remote Access Service Provider, the PPP login ID should contain information in the following format: *secureip.X.Y*, where *secureip* is your service, *X* is your account name, and *Y* is your user ID.

**Note:** For the SNMP over LAN and SNMP over PPP notification methods to work properly, configure the SNMP options on the Network Interfaces/Protocols window. For more information on SNMP, see "Configuring SMTP" on page 49.

12. If you select the E-mail over PPP or SNMP over PPP notification methods, type the password that accompanies the login ID in the PPP Password field.

Enter the password needed to login to the dial-up service account. You must fill in this field for the E-mail over PPP and SNMP over PPP notification methods.

13. If you select the E-mail over LAN or E-mail over PPP notification methods, type the e-mail address for the recipient in the E-mail Address field.

**Note:** For the E-mail over LAN and E-mail over PPP notification methods to work properly, configure the SMTP options on the Network Interfaces/Protocols window.

14. Press F3 twice to return to the Login and Alert Profiles window.

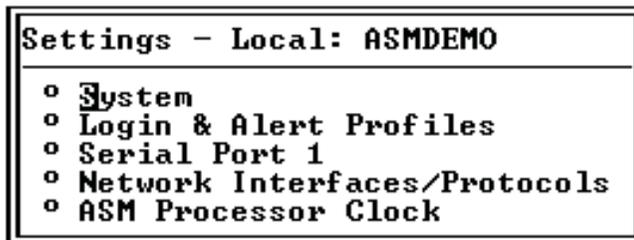
Continue with the “Setting remote alert attempts” procedure.

---

## Setting remote alert attempts

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

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 53.
2. In the Advanced System Management window, select **Settings**. The Settings window opens:



3. Select **Login & Alert Profiles**.

4. From the Login & Alert Profiles window, select **Remote Alert Settings**.

Use these settings to define the number of remote alert attempts and the time between the attempts.

5. In the Remote Alert Retry Limit field, specify the number of additional times that the Remote Supervisor Adapter will attempt to forward an alert to an alphanumeric pager. All other notification methods are attempted only once.
6. In the Delay Between Retries field, specify the time interval (in minutes) that the Remote Supervisor Adapter will wait between retries to send an alert.
7. In the Include event log with e-mail alerts? field, select **Yes** or **No**.

You can attach detailed information to alert recipients who are set up to receive e-mail as their notification method. The event log provides a summary of the most recent event and assists with problem identification and fast recovery.

**Notes:**

- a. To send the event log as an e-mail attachment, you must select **E-mail over LAN** or **E-mail over PPP** as the notification method for at least one remote alert recipient.
  - b. Event logs attached to an e-mail are not forwarded to a Remote Supervisor Adapter on the ASM interconnect network.
8. Press F3 to return to the Login & Alert Profiles window.

Continue with the “Setting remote alerts” on page 67 procedure.

---

## Setting remote alerts

Complete the following steps to select which remote alerts are to be sent by the Remote Supervisor Adapter:

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 53.
2. In the Advanced System Management window, select **Settings**. The Settings window opens:

```
Settings - Local: ASMDEMO
  o System
  o Login & Alert Profiles
  o Serial Port 1
  o Network Interfaces/Protocols
  o ASM Processor Clock
```

3. Select **Login & Alert Profiles**.
4. In the Login and Alert Profiles window, select Critical/Warning Remote Alerts.

```
Critical/Warning Remote Alerts - Local: ASMDEMO

  Critical Alerts
  -----
Hard Disk Drive:          <Disabled>
Multiple Fan Failure:    <Disabled>
Power Failure:           <Disabled>
Tamper:                  <Disabled>
Temperature:             <Disabled>
Voltage:                 <Disabled>
URM Failure:             <Disabled>

  Warning Alerts
  -----
Single Fan Failure:      <Disabled>
Non-Critical Temperature: <Disabled>
Non-Critical Voltage:   <Disabled>
Redundant Power Supply: <Disabled>
```

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

- Critical
- Warning
- System

All alerts are tracked 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. You can select the **Select all critical alerts** check box to be alerted with any event.

Table 15. Critical remote alerts.

| Event                      | Action                                                                                                                                                                                                                                                                                                                                                                | Numeric code |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| Hard disk drive failure    | Generates an alert if one or more of the hard disk drives in the system fail.                                                                                                                                                                                                                                                                                         | 05           |
| Multiple fan failure       | Generates an alert if two or more of the cooling fans in the system fail.                                                                                                                                                                                                                                                                                             | 03           |
| Power failure              | Generates an alert if any of the system power supplies fail.                                                                                                                                                                                                                                                                                                          | 04           |
| 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.                                                                                                                                                                                                    | 02           |
| Temperature irregularities | Generates an alert if any of the monitored temperatures are outside critical threshold values. These threshold values can be found by clicking the temperature readings on the System Health page. If a critical temperature condition is detected, the server will automatically shut down and turn off whether this field is selected or not.                       | 00           |
| Voltage irregularities     | Generates an alert if the voltages of any of the monitored power supplies fall outside their specified operational ranges. These operational ranges are accessed by clicking the voltage readings on the System Health page. If a critical voltage condition is detected, the server will automatically shut down and turn off whether this field is selected or not. | 01           |
| VRM failure                | Generates an alert if one or more VRMs fail. VRMs are not used on some servers, in which case this setting is ignored.                                                                                                                                                                                                                                                | 06           |

#### Warning alerts

Warning alerts are generated for events that might progress to a critical/error level.

Table 16. Warning remote alerts.

| Event                          | Action                                                                                                                                                                                                                                                                                                       | Numeric code |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| Single fan failure             | Generates an alert if one fan fails.                                                                                                                                                                                                                                                                         | 11           |
| Temperature irregularities     | Generates an alert if any monitored temperatures are outside the warning threshold values. These temperature threshold values are accessed by clicking the temperature readings on the System Health page. Unlike the critical temperature event, this event will not initiate an automatic system shutdown. | 12           |
| Voltage irregularities         | Generates an alert if any monitored voltages are outside the warning threshold values. These voltage range values are accessed by clicking the voltage readings on the System Health page. Unlike the critical voltage event, this event will not initiate an automatic system shutdown.                     | 13           |
| Redundant power supply failure | Generates an alert if a redundant power supply fails.                                                                                                                                                                                                                                                        | 10           |

**Note:** Hard disk drive Predictive Failure Analysis<sup>®</sup> (PFA) alerts are not monitored.

- Press F3 and select **System Remote Alerts**.

#### System alerts

System alerts are generated for events that occur as a result of system errors.

Table 17. System remote alerts.

| Event            | Action                                                                                                                                                                                                                                                    | Numeric code |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| Boot failure     | Generates an alert if an error occurred that prevented the system from starting.                                                                                                                                                                          | 25           |
| Loader timeout   | Generates an alert if a system loader timeout value is enabled and has been exceeded. The system loader timeout value is configured in the Server Timeouts section on the System page.                                                                    | 26           |
| O/S timeout      | Generates an alert if the operating system timeout value is enabled and has been exceeded. The operating system timeout value is configured in the Server Timeouts section on the System page. This alert must be checked for remote blue screen capture. | 21           |
| PFA notification | Generates an alert if a PFA notification is generated by the system hardware. This feature is available only on systems that have PFA-enabled hardware. This setting is ignored by systems without PFA-enabled hardware.                                  | 27           |
| POST timeout     | Generates an alert if the POST timeout value is enabled and has been exceeded. The POST timeout value is configured in the Server Timeouts section on the System page.                                                                                    | 20           |
| Power off        | Generates an alert if the system is turned off.                                                                                                                                                                                                           | 23           |
| Power on         | Generates an alert if the system is turned on.                                                                                                                                                                                                            | 24           |

6. Press F3 and select **Events For Local Notification**.
7. Select the events that you want to store in the event log. The Remote Supervisor Adapter stores the notification only in the event log.

**Local events**

Eventually, local events will be sent to the server where the Remote Supervisor Adapter resides. These events will not be sent to remote alert recipients.

Table 18. Local events.

| Event                  | Action                                                                                                              |
|------------------------|---------------------------------------------------------------------------------------------------------------------|
| Temperature            | Generates a local notification if any of the monitored temperatures exceeds threshold.                              |
| Voltage                | Generates a local notification if any of the monitored voltages exceeds their threshold.                            |
| Redundant power supply | Generates a local notification if the redundant power supply fails.                                                 |
| Power off              | Generates a local notification if the server is turned off.                                                         |
| Remote login           | Generates a local notification if a remote login occurs.                                                            |
| System tamper          | Generates a local notification if the server covers are removed. This feature is only available on certain servers. |
| Event log 75% full     | Generates a local notification if the event log reaches 75% of capacity.                                            |
| Event log full         | Generates a local notification if the event log fills. When the event log fills, the oldest events are deleted.     |
| Fan failure            | Generates a local notification if one or more cooling fans fails.                                                   |
| Power supply failure   | Generates a local notification if a power supply failure is detected.                                               |
| DASD failure           | Generates a local notification if any hard disk drive failure is detected.                                          |

Table 18. Local events.

| Event | Action                                                                               |
|-------|--------------------------------------------------------------------------------------|
| PFA   | Generates a local notification if any of the hardware in the system generates a PFA. |

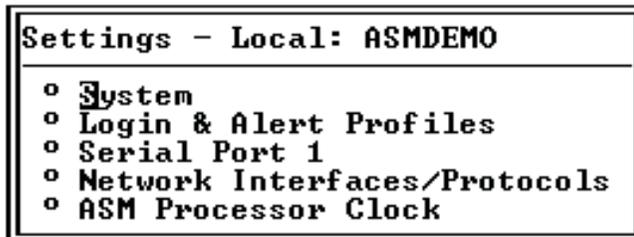
## Configuring the serial port

You can either dedicate the integrated serial port on the Remote Supervisor Adapter to system management or share it with the server operating system. If dedicated to system management, the serial port serves only the Remote Supervisor Adapter and is always available for dial-in and dial-out alerting purposes. You will not be able to view the port on the network operating system (NOS) or in any other applications.

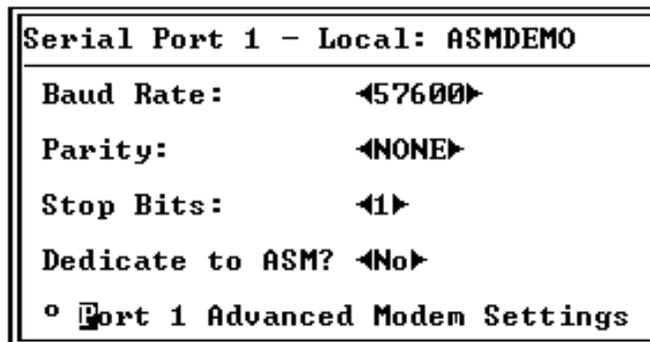
This design enables a single modem to conduct normal functions and also maintain out-of-band alerting capabilities.

Complete the following steps to configure your serial port. For more information on your serial port, see “Configuring PPP access over the serial port” on page 75.

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 53.
2. In the Advanced System Management window, select **Settings**. The Settings window opens:



3. In the settings window, select **Serial Port 1**.



4. In the Baud Rate field, select a data transfer rate.  
The baud rate specifies 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 use in your serial connection.

The parity value specifies the error detection bit 0 or 1 added to each group of transmitted bits so that it will have either an odd or even number of 1s. This enables your server to know whether received data has been corrupted during transmission.

6. Select the number of data-terminating 1-bits that will follow the data or any parity bit to mark the end of a transmission.

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

The stop bits value specifies how many extra 1-bits follow the data and any parity bit to mark the end of a unit of transmission (normally a byte or character).

7. In the Dedicate to ASM field, select **Yes** to reserve the serial port for the Remote Supervisor Adapter.

If shared with the operating system, the serial port serves the Remote Supervisor Adapter when the server is turned off or if it is turned on during the power-on self-test (POST). The operating system can access it after the POST completes. Only after a critical event will the Remote Supervisor Adapter take over the port from the NOS to dial-out and transmit an alert. The port then remains under the Remote Supervisor Adapter control until the server is restarted.

**Note:** If a PPP interface is configured, dedicate the serial port to the Remote Supervisor Adapter or the PPP port will be lost when the host restarts.

8. If you need to set advanced settings, select **Port 1 Advanced Modem Settings**.

Set these values only if the alert forwarding functions are not working properly. The strings marked with an asterisk (\*) require a carriage return (^M) to be manually entered at the end of the field value.

The following table describes the initialization strings for this modem.

Table 19. Port 1 settings.

| Field                                 | What you enter                                                                                                                                                                                    |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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. |
| Caller ID string                      | Type the initialization string that will be used to get caller ID information from the modem.                                                                                                     |
| 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.                                                                |
| Escape guard (1 - 250 10ms Intervals) | Type the length of time before and after the escape string is issued to the modem. This value is measured in 10 millisecond intervals. The default value is 1 second.                             |
| Escape string                         | Type the initialization string that returns the modem to command mode when it is currently talking to another modem. The default is +++.                                                          |
| Dial prefix string                    | Type the initialization string that is used before the number to be dialed. The default is ATDT.                                                                                                  |
| 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.                                                                      |
| 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 two rings or ATSO=1.                                              |
| 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 ATSO=0.                                                     |
| Modem query                           | Type the initialization string that is used to find out if the modem is attached. The default is AT.                                                                                              |

Table 19. Port 1 settings.

| Field         | What you enter                                                                                                                                                                                               |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 dialout functions are not working properly. |

---

## Initialization-string guidelines

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

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

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

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

---

## Configuring network interfaces

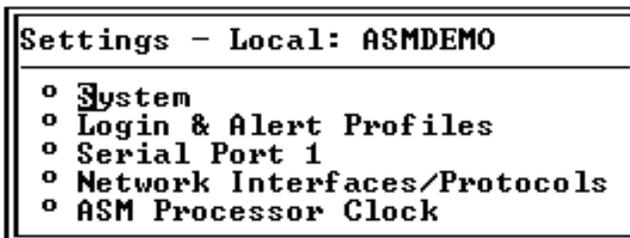
With the network interface options, you can set access to the Remote Supervisor Adapter by:

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

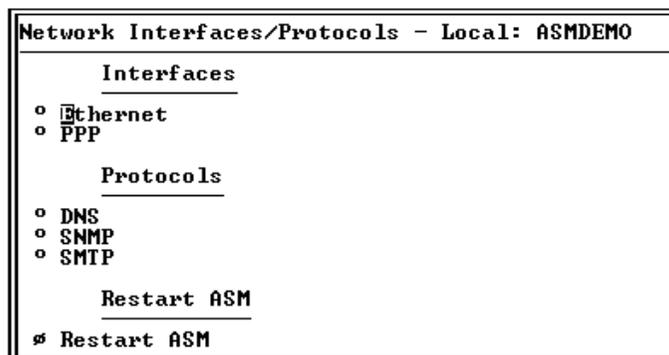
### Configuring an Ethernet connection to ASM

Complete the following steps to configure your Ethernet setup:

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 53.
2. In the Advanced System Management window, select **Settings**. The Settings window opens:

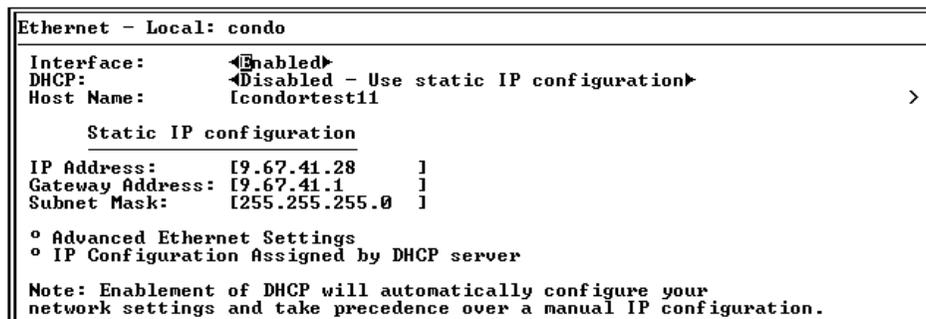


3. In the Settings window, select **Network Interfaces/Protocols**. The following window opens:



4. Select **Ethernet**. A window similar to the following opens.

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



5. In the Interface field, select **Enabled**. It is enabled by default.
6. If you want to use a dynamic host configuration protocol (DHCP) server connection, enable the DHCP field and then go to step 11.

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

7. Type the IP host name of the Remote Supervisor Adapter in the Host Name field. This step is only necessary if you disabled DHCP.

You can enter a maximum of 63 characters in this field, which represents the IP hostname of the Remote Supervisor Adapter. The hostname by default is "ASMA" followed by the burned-in MAC address of the server in which the ASM is installed.

**Notes:**

- a. The IP host name of the Remote Supervisor Adapter (the Host Name field) and Remote Supervisor Adapter 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 while the Host Name field can consist of up to 63 characters. To minimize confusion, set the ASM Name field to the non-qualified portion of the IP hostname. The non-qualified IP hostname consists of up to the first period of a fully qualified IP hostname. For example, the non-qualified IP hostname of asmcard1.us.company.com (a fully qualified IP hostname) is asmcard1. For more information on your hostname, see “Setting system information” on page 57.
- b. If DHCP is enabled, the Host name field is used as follows:
  - If the **Hostname** field is set, then the Remote Supervisor Adapter DHCP support will request that the DHCP server use this hostname.
  - If the **Hostname** field is not set, then the Remote Supervisor Adapter DHCP support will request that the DHCP server assign a unique hostname to the Remote Supervisor Adapter.
8. In the IP Address field, type the IP address of the Remote Supervisor Adapter. This step is only necessary if you disabled DHCP. The IP address must contain:
  - Four integers from 0 to 255 separated by periods
  - No spaces
9. In the Gateway Address field, type your network gateway router. This step is only necessary if you disabled DHCP. The gateway address must contain:
  - Four integers from 0 to 255 separated by periods
  - No spaces or consecutive periods
10. In the Subnet Mask field, type the subnet mask used by the Remote Supervisor Adapter. This step is only necessary if you disabled DHCP. The subnet mask must contain:
  - Four integers from 0 to 255 separated by periods
  - No spaces or consecutive periodsThe default setting is 255.255.255.0.
11. Select **Advanced Ethernet Settings** if you need to set additional Ethernet settings. Make modifications as necessary.

```
Advanced Ethernet Settings - Local: condortest11
Data Rate:                               <Auto>
Duplex:                                   <Auto>
Maximum Transmission Unit <60-1500>: [1500]
Locally Administered MAC Address: [00:00:00:00:00:00]

Note: The Burned-In MAC address takes precedence when the
Locally Administered MAC Address is 00:00:00:00:00:00
Burned-In MAC Address:                 00:02:55:38:07:56
```

Table 20. Advanced Ethernet setup.

| Field                               | Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data rate                           | <p>Use the Data Rate field to specify the amount of data to be transferred per second over your LAN connection.</p> <p>To set the data rate, select the data transfer rate in megabits (Mb) that corresponds to your network capability. To automatically detect the data transfer rate, select Auto, which is the default value.</p>                                                                                                                                                                                                                                                                                |
| Duplex                              | <p>Use the Duplex field to specify the type of communication channel used in your network.</p> <p>To set the duplex mode, select one of the following:</p> <p><b>Full</b> Enables data to be carried in both directions at once.</p> <p><b>Half</b> Enables data to be carried in either one direction or the other, but not both at the same time.</p> <p>To automatically detect the duplex type, select Auto, which is the default value.</p>                                                                                                                                                                     |
| Maximum transmission unit <60-1500> | <p>Use this field to specify the maximum size of a packet (in bytes) for your network interface. For Ethernet, the valid maximum transmission unit (MTU) range is 60 - 1500. The default value for this field is 1500.</p>                                                                                                                                                                                                                                                                                                                                                                                           |
| Locally administered MAC address    | <p>Enter a physical address for this Remote Supervisor Adapter 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 between 000000000000 - FFFFFFFF. This value must be in the form XX:XX:XX:XX:XX:XX where X is a number between 0 and 9. The Remote Supervisor Adapter does not support the use of a multicast address. A multicast address has the least significant bit of the first byte set to 1. The first byte, therefore, must be an even number.</p> |
| Burned-in MAC address               | <p>The burned-in MAC address is a unique physical address assigned to this Remote Supervisor Adapter by the manufacturer. The address is also a read-only field.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

12. Select **IP Configuration Assigned by DHCP server** to view the current configuration. It is enabled by default. A table opens that lists the IP address, gateway address, and subnet mask set by the DHCP server, as well as the server host name.
 

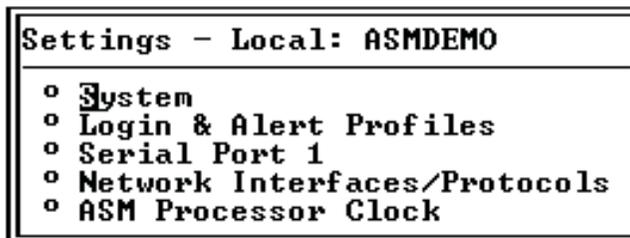
If DHCP is enabled, the hostname, IP address, gateway address, subnet mask, and DNS server IP address will be set automatically.
13. Press F3 until you reach the Network Interfaces/Protocols window and then select **Restart ASM**.

## Configuring PPP access over the serial port

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 through a TELNET session or a Web browser.

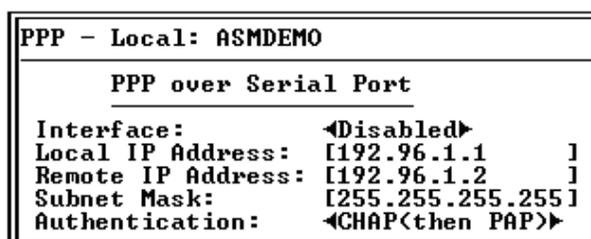
**Note:** If you enable the PPP interface, the Remote Supervisor Adapter cannot use the serial port for serial remote access.

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 53.
2. In the Advanced System Management window, select **Settings**. The Settings window opens:



3. In the Settings window, select **Network Interfaces/Protocols**.
4. In the Network Interfaces/Protocols window, select **PPP**. The PPP window opens:

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



5. In the Interface field, select **Enabled**.
6. In the Local IP address field, enter the local address for the PPP interface on this Remote Supervisor Adapter. The field defaults to 192.96.1.1. The IP address must contain:
  - Four integers from 0 to 255 separated by periods
  - No spaces
7. In the Remote IP Address field, enter the remote IP address that this Remote Supervisor Adapter will assign to a remote user. The field defaults to 192.96.1.2. The remote IP address must contain:
  - Four integers from 0 to 255 separated by periods
  - No spaces
8. In the Subnet Mask field, enter the subnet mask that will be used by the Remote Supervisor Adapter. The default is 255.255.255.255. The subnet mask must contain:
  - Four integers from 0 to 255 separated by periods
  - No spaces
9. 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 a connection. This weaker 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. This authentication protocol is stronger than the PAP Only setting 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 will be tried as a secondary authentication protocol. The **CHAP (then PAP)** setting is the default.
10. Press F3 until you return to the Network Interfaces/Protocols window, and then select the **Restart ASM** option.

---

## Configuring network protocols

With the network protocols options, you can perform the following functions:

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

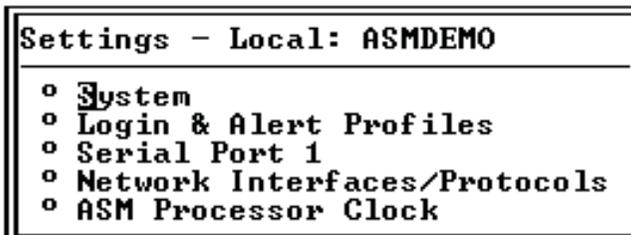
## Configuring SNMP

The simple network management protocol (SNMP) enables you to 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 are planning to configure SNMP trap alerts on the Remote Supervisor Adapter, you must install and compile the supplied management information base (MIB) on your SNMP manager. For more information on the MIB file, see your *Remote Supervisor Adapter Installation Guide*.

Complete the following steps to configure your SNMP:

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 53.
2. In the Advanced System Management window, select **Settings**. The Settings window opens:



3. From the Settings window, select **System** and enter your system contact and system location information. For more information on the system settings, see “Setting system information” on page 57.

If these fields are already configured, return to the Network Interfaces/Protocols window and continue with the next step.

4. From the Settings window, select **Network Interfaces/Protocols**.
5. Select the **SNMP** option. The SNMP window opens:

```

SNMP - Local: ASMDEMO
-----
Simple Network Management Protocol
-----
SNMP Agent: <Disabled>
SNMP Traps: <Enabled>

o Community 1
o Community 2
o Community 3

```

6. Enable the SNMP Agent and SNMP Traps fields.

Enabling the SNMP Agent field forwards alerts to SNMP communities on your network. To enable the SNMP agent, the following criteria must be met:

- System contacts must be specified in the System window.
- System location must be specified in the System window.
- At least one community name specified.
- At least one valid IP address or hostname (if DNS is enabled) must be specified for that community.

Alert recipients whose notification method is SNMP do not receive alerts unless both the SNMP Agent and SNMP Traps fields are enabled.

7. Select a community option. A Community window opens:

```

Community 1 - Local: ASMDEMO
-----
Name: [ ]
Host Name1 or IP Address1: [ ]
Host Name2 or IP Address2: [ ]
Host Name3 or IP Address3: [ ]

```

You need to 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
- Host name or IP address

If any of these parameters are not correct, you will not be granted SNMP management access.

8. In the Name field, enter the name or authentication string that corresponds to the desired community.
9. In the corresponding Host Name1 or IP Address1 field for this community, type the host name or IP addresses of this community.
10. Press F3 until you return to the Network Interfaces/Protocols window.

## Configuring DNS

Use this option to specify whether you use a Domain Name System (DNS) server on your network to translate host names into IP addresses.

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 53.
2. In the Network Interfaces/Protocols window, select **DNS**. A window similar to the following opens:

```

DNS - Local: condortest11
-----
Domain Name System
DNS Status: <Enabled>
DNS Server IP Address 1: [9.37.0.5 ]
DNS Server IP Address 2: [9.37.0.6 ]
DNS Server IP Address 3: [0.0.0.0 ]

Host Table <IP Address to Host Name Mappings>
-----
Host Name 1: [ ] >
Host IP Address 1: [0.0.0.0 ]
Host Name 2: [ ] >
Host IP Address 2: [0.0.0.0 ]
Host Name 3: [ ] >
Host IP Address 3: [0.0.0.0 ]
Host Name 4: [ ] >
Host IP Address 4: [0.0.0.0 ]

```

3. In the DNS Status field, enable the DNS.  
The DNS Status field specifies whether you use a DNS server on your network to translate host names into IP addresses.
4. In the DNS Server IP Address fields, enter the IP address of up to three DNS servers if DNS is enabled. You only need to do this if a quick lookup of a host name IP address is required.  
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 to 255, separated by periods.
5. In the Host Table section, enter a host name and its corresponding IP address. You can define four mappings.  
Use the fields in the Host Table section to define relationships between an IP address and its corresponding host name in the event that your network DNS server is unreachable. You can also use these mappings for frequently used hostnames.  
**Note:** The Remote Supervisor Adapter uses this table first when searching for an address to host name mapping. If a match is not found, the data will be requested from the DNS server. If the table contains an entry for a given address, the host name defined in the table will override any corresponding entry defined on the DNS server.
6. Press F3 until you return to the Network Interfaces/Protocols window.

## Configuring SMTP

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

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 53.
2. In the Network Interfaces/Protocols window, select **SMTP**. The SMTP window opens:

```

SMTP - Local: ASMDemo
-----
Simple Mail Transfer Protocol
SMTP Server Host Name or IP Address: [ ]

```

3. Enter the hostname of the SMTP server in the SMTP Server Host Name or IP Address field. This field must be defined to enable e-mail alerts to be sent.

4. Press F3 until you return to the Network Interfaces/Protocols window, and then select **Restart ASM**.

---

## Setting the Remote Supervisor Adapter clock

Complete the following steps to set the Remote Supervisor Adapter clock:

1. In the Advanced System Management window, select **Settings**.
2. In the Settings window, select the **ASM Processor Clock**, which shows the date and time when this window was generated. Use this information to check the settings of the date and time processor on the Remote Supervisor Adapter, which is independent of the date and time settings of the clock on the server system board.

The Remote Supervisor Adapter has a clock that timestamps all events that are logged in the battery-backed 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 battery-backed event log, even if the system is turned off or disabled. This facilitates immediate problem determination and resolution.

3. To set the time, type the current hour, minutes, and seconds in the matching text boxes. 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.
4. Set the time zone settings, depending on your location.

### **GMT offset**

Use the Offset from GMT field to specify the time difference from GMT corresponding to the time zone where this server is located.

### **Daylight Savings Time**

Use the Observe daylight savings time field to specify whether the Remote Supervisor Adapter clock will adjust when DST changes.

5. Press **F6** to save your changes.

## Chapter 8. The text-based Interfaced system health and tasks

Use the options under the Monitors heading in the Advanced System Management window to view the status of the server that you want to access.

**Note:** F1 through F4 are the only function keys that are supported in the text-based interface.

### Monitoring temperatures, voltage, and fan readings

Complete the following steps to access the temperature, voltage, and fan readings of the remote server. The Remote Supervisor Adapter tracks the current temperature readings and threshold levels for system components such as microprocessors, the system board, and the hard disk drive backplane.

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 53.
2. Select **Temperature, Voltage and Fan**. A window similar to the following opens:

```
Temperature, Voltage and Fan - Local: ASMDemo
-----
System Power Status: Off
Power On Hours: 0
Reboot Count: 0
System State: System power off/State unknown

These tables will take a few moments to process:
o Temperature Tables
o Voltage Tables
o Fan Table
```

3. Select the **Temperature Tables** option. A window similar to the following opens:

```
Temperature Tables - Local: ASMDemo
-----
o CPU Temperatures
o Dasd Temperatures
o System Temperatures
```

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

#### Warning

When a temperature reaches a certain value, a temperature warning is sent to remote alert recipients if set in the Critical/Warning Remote Alerts window. For more information on setting the Temperature option, see “Configuring terminal settings” on page 54.

#### Soft Shutdown

When a temperature reaches a certain value higher than the warning value, a second temperature warning is sent to remote alert recipients (if set in the Critical/Warning Remote Alerts window) and the system begins the shutdown process with an orderly operating-system shutdown followed by a power off.

### Hard Shutdown

When a temperature reaches a certain value higher than the soft shutdown value, the system immediately shuts down and sends an alert to configured recipients (if set in the Critical/Warning Remote Alerts window).

### Warning Reset

When the temperature returns to a value below the warning reset value after a warning was sent, the system assumes the temperature has returned to normal and no further alerts are generated.

4. Select **Voltage Tables**. The Remote Supervisor Adapter will send an alert if any monitored power source voltage falls outside its specified operational ranges. The system displays the voltage readings of the system board (planar) and the voltage regulation modules (VRM).

The voltage tables windows display the voltage ranges at which the Remote Supervisor Adapter reacts. These levels are preset on the remote server and cannot be changed. The system sets a voltage range at which the following actions are taken:

### Warning

When the voltage drops below or exceeds a specific voltage range, a voltage warning is sent to remote alert recipients if set in the Critical/Warning Remote Alerts window. For more information on setting the Temperature option, see “Configuring remote alert recipients” on page 63.

### Soft Shutdown

When the voltage drops below or exceeds a specific voltage range, a voltage warning is sent to remote alert recipients (if set in the Critical/Warning Remote Alerts window) and the system begins the shutdown process with an orderly operating-system shutdown followed by a power off.

### Hard Shutdown

When the voltage drops below or exceeds a specific voltage range, the system immediately shuts down and sends an alert to configured recipients (if set in the Critical/Warning Remote Alerts window).

### Warning Reset

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

5. Select **Fan Table**. The Fan Speeds window displays the running speed of the system fans (converted to a percentage of the maximum fan speed). A fan warning (Multiple Fan Failure or Single Fan Failure) is sent if the fan drops to an unacceptable speed or stops.

---

## Viewing the event log

The Event Log window displays the system error log and POST error log two entries at a time. Information about all remote access attempts and dial-out events are recorded in the adapter event log. The Remote Supervisor Adapter time stamps all events and logs them into the event log, sending out the appropriate alerts if configured to do so by the system administrator.

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 53.
2. In the Advanced System Management window, select **Event Log**.
3. Select **View Event Log** to view the two most recent events on your server.

```

View Event Log - Local: ASMDEMO
-----
Date:01-01-00 Time:04:14:37 Severity:I Source:SERUPROC
TCP connection reset by other host.
Date:01-01-00 Time:04:07:45 Severity:I Source:SERUPROC
Remote Login Successful. Login ID: guest2
-----
o View next log entry.

```

The events are given the following levels of severity:

**I (information)**

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

**W (warning)**

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

**E (error)** This severity level is assigned to an event that needs immediate attention.

4. Select **View next log entry** to view the next two entries.

## Viewing vital product data

Upon server startup, the Remote Supervisor Adapter collects system, BIOS code, and server component Vital Product Data (VPD) and stores it in nonvolatile memory. You can access this information at any time from anywhere. The vital product data option contains key information about the system that the Remote Supervisor Adapter is monitoring.

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 53.
2. In the Advanced System Management window, select **System Information** to view the status of the hardware and software components on the server.
3. Select **Vital Product Data (VPD)**. The Vital Product Data windows opens:

```

Vital Product Data <VPD> - Local: ASMDEMO
-----
o Machine Level VPD
o Component Level VPD
o POST/BIOS VPD
o ASM VPD

```

4. Select the option corresponding to the information you want:

**Machine level VPD**

The VPD for the system is displayed in this window.

Table 21. Machine level vital product data.

| Field         | Function                                                                               |
|---------------|----------------------------------------------------------------------------------------|
| Machine type  | Identifies the type of server the Remote Supervisor Adapter is monitoring.             |
| Machine model | Identifies the model number of the server the Remote Supervisor Adapter is monitoring. |

Table 21. Machine level vital product data.

| Field         | Function                                                                                |
|---------------|-----------------------------------------------------------------------------------------|
| Serial number | Identifies the serial number of the server the Remote Supervisor Adapter is monitoring. |

#### Component level VPD

The VPD for the system components is displayed in this window.

Table 22. Component level vital product data.

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

#### POST/BIOS data

You can find the VPD for the system POST or BIOS firmware code in this window.

Table 23. POST/BIOS vital product data.

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

#### Power backplane data

You can find the VPD for the system power backplane firmware code in this window.

Table 24. Power Backplane vital product data.

| Field             | Function                                                        |
|-------------------|-----------------------------------------------------------------|
| Firmware revision | Identifies the revision number of the power backplane firmware. |

#### Remote Supervisor Adapter system data

You can find the VPD for the Remote Supervisor Adapter in this section.

Table 25. Remote Supervisor Adapter vital product data.

| Field    | Function                                                                               |
|----------|----------------------------------------------------------------------------------------|
| Build ID | Identifies the build ID of both the application firmware and the startup ROM firmware. |

Table 25. Remote Supervisor Adapter vital product data.

| Field        | Function                                                                                      |
|--------------|-----------------------------------------------------------------------------------------------|
| Revision     | Identifies the revision number of both the application firmware and the startup ROM firmware. |
| File name    | Identifies the file name of both the application firmware and the startup ROM firmware.       |
| Release date | Identifies the release date of both the application firmware and the startup ROM firmware.    |

#### Integrated System Management Processor data

You can find the VPD for the integrated System Management processor firmware code in this window.

Table 26. Integrated System Management Processor vital product data.

| Field             | Function                                                                               |
|-------------------|----------------------------------------------------------------------------------------|
| Firmware revision | Identifies the revision number of the integrated System Management processor firmware. |

- Press F3 to return to the System Information window.

#### Component Activity Log

You can find a record of component activity.

Table 27. Component activity log.

| Field           | Function                                                                                                                                          |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| FRU number      | Identifies the field replaceable unit (FRU) number (a seven-digit alphanumeric number) 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. |

- Press F3 to return to the System Information window.

---

## Performing Remote Supervisor Adapter tasks through a text-based interface

The functions under the Tasks heading in the Advanced System Management window enable you to directly control the actions of the Remote Supervisor Adapter and your server.

**Note:** F1 through F4 are the only function keys that are supported in the text-based interface.

## Remotely controlling the power status of a server

**Attention:** You must have the UM Server Extensions code installed to enable an orderly operating system shutdown. If you do not have the UM Server Extensions code installed, the server turns off after waiting for the length of time you set in the Power Off Delay field. You could lose or damage data on your server. For more information on installing UM Server Extensions code for the Remote Supervisor Adapter, see your *UM Server Extensions User's Guide*.

The Remote Supervisor Adapter 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. Select the following options only in case of an emergency, or if you are offsite and the server is nonresponsive:

### **Power on server immediately**

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

### **Power off server immediately**

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

### **Shutdown O/S and then power off server**

To shut down the operating system and then turn off this server, select the **Shutdown O/S and then Power Off Server** option. This option requires that the IBM System Management device driver be installed on the server, as well as IBM Director with UM Server Extensions for the ASM component.

### **Shutdown O/S and then restart server**

To restart the operating system, select the **Shutdown O/S and then Restart Server** option. This option requires that the ASM Device Driver be installed on the server, as well as IBM Director with UM Server Extensions for the ASM component.

### **Restart the server immediately**

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

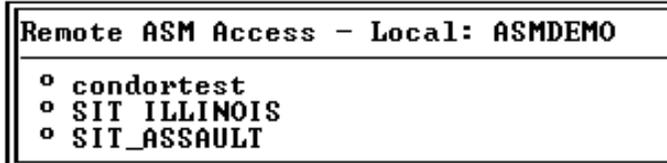
To perform any of these actions, you must have read/write access to the Remote Supervisor Adapter. With the operating system shutdown options, the Remote Supervisor Adapter communicates with the system-management software through the device driver and the system-management software initiates the shutdown.

## Accessing remote adapters through ASM interconnect network

You can connect to remote systems through the ASM interconnect network on the Access Remote ASM window. The Remote ASM Access table indicates the overall status of each remote server in the System Health column using color-coded icons. The server name is the name corresponding to each remote system.

Complete the following steps to access remote Remote Supervisor Adapters:

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 53.
2. In the Advanced System Management window, select **Remote ASM Access**. The Remote ASM Access window opens, listing other system-management adapters and processors linked to the host server.



3. Select a processor or adapter. The Remote ASM Login window opens.
4. Enter your user name and password.  
**Note:** It might take up to 45 seconds for newly attached servers to be reflected in the table of available remote systems. It might take up to 2 minutes for systems to be removed from the table when detached from the ASM interconnect network.
5. The ASM window opens, giving you access to the remote system management adapter or processor.  
**Note:** Depending on the adapter on the remote server, some options might not be available.

## Viewing remote POST

When the Remote Video option is selected, the Remote Video window opens. Characters that are visible on the full screen text display of the server are displayed in the Remote Video window. The Remote Video window does not display information from the server when the server video is set to graphics mode. The Remote Video option does not automatically restart the server when it is selected.

Note the following about the text-based interface:

- The function keys that are supported are only F1 through F4.
- The window viewing area is 80 characters x 24 lines.

Complete the following steps to remotely view a server POST.

1. Restart the server. For more information, see "Remotely controlling the power status of a server" on page 86.
2. Press F3 to return to the Advanced System Management window.
3. Select **Remote Video**. The Remote Video window opens and the text that is displayed during the server POST displays on your screen.
4. Press Ctrl R+E+T to return to the Advanced System Management window.  
**Note:** After you close the Remote Video window, if you return to the server POST by again selecting the Remote Video option, characters that are visible on the full screen text display of the server are displayed again in the Remote Video window.

## Powering on or restarting servers

The following links enable you to restore the Remote Supervisor Adapter if you have read/write access.

1. Click **Server Power/Restart** for options on restarting the Remote Supervisor Adapter.
2. Click **Restore Defaults** to refresh the Remote Supervisor Adapter. Your TCP/IP or modem connections will be broken and you will need to login again to use the ASM Web interface.

**Attention:** When you select the **Restore ASM to Factory Defaults** option, you will lose all the modifications you made to the Remote Supervisor Adapter. You also lose remote control of the remote servers. You will have to reset the password locally on the remote servers during BIOS setup.

## Viewing the server text console

From the Redirect Text Console menu, select **Redirect Text Console** to view an interactive text display of the server. This option allows you to see on your monitor exactly what you would see on the server monitor, and have full keyboard and mouse control of the desktop. Selecting the redirect text console does not restart the server.

Complete the following steps to remotely access the text console of the server:

1. Click **Remote Control** on the navigation frame.
2. Click the **Redirect Text Console** button to access the server text console. A Java applet launches in a separate browser window.
3. Enter the remote control password. This password is configured locally on the server during the BIOS code update.
4. A telnet session opens, displaying the server text console on your screen.

You can disconnect at any time by closing the applet window.

### Configuring special keys

During server console redirect and remote POST, keyboard support is limited to ASCII characters, the arrow keys, and the F1 through F12 function keys. To transmit certain special key combinations, such as Ctrl+Alt+Del on Microsoft Windows® operating systems, you must type a prefix key combination followed by a second key as described on the Configuring Special Keys menu. You can define the prefix key combination that you want to use, as indicated on the Configuring Special Keys menu. The default prefix key combination is Ctrl+].

Complete the following steps to configure prefix key combinations.

1. From the Redirect Text Console menu, select **Configure Special Keys**. The Configure Special Keys window opens.
2. Follow the directions in the window to select and save the desired prefix key combination.

## Restoring ASM to factory defaults

The following option enables you to restore the Remote Supervisor Adapter settings if you have read/write access.

**Attention:** When you select the **Restore ASM to Factory Defaults** option, you will lose all the modifications you made to the Remote Supervisor Adapter. You also lose remote control of the remote servers. You will have to reset the password locally on the remote servers during BIOS setup.

Select the **Restore ASM To Factory Defaults** option in the Advanced System Management window to reset the Remote Supervisor Adapter to its original factory settings. You will lose your TCP/IP connection and must reconfigure the network interface.

## Restarting ASM

The following option enables you to restart the Remote Supervisor Adapter if you have read/write access.

**Attention:** When you select the Restart ASM option, you will lose all the modifications you made to the Remote Supervisor Adapter. You also lose the remote control of the remote servers. You will have to reset the password locally on the remote servers during BIOS setup.

Select the **Restart ASM** option in the Advanced System Management window. Your TCP/IP or modem connections will be broken and you will need to login again to use the ASM Web interface.

## Logging off

Complete the following steps to log off the Remote Supervisor Adapter:

1. In the Advanced System Management window, select **Log Off**.
2. Click **Yes**.



---

## Appendix A. Getting information, help, and service

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 section contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your computer, and whom to call for service should it be necessary.

---

### Getting information

Information about your IBM server product and preinstalled software, if any, is available in the documentation that comes with your server. That documentation includes printed books, online books, README files, and help files. In addition, information about IBM products is available on the World Wide Web and through the IBM Automated Fax System.

### Using the World Wide Web

On the World Wide Web, the IBM Web site has up-to-date information about IBM products and support. The address for the IBM Personal Computing home page is <http://www.ibm.com/pc/>.

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

If you click **Profile** from the support page, you can create a customized support page that is specific to your hardware, complete with Frequently Asked Questions, Parts Information, Technical Hints and Tips, and Downloadable Files. In addition, you can choose to receive e-mail notifications whenever new information becomes available about your registered products.

You also can order publications through the IBM Publications Ordering System at <http://www.elink.ibm.com/public/applications/publications/cgibin/pbi.cgi>.

### Getting information by fax

If you have a touch-tone telephone and access to a fax machine, in the U.S. and Canada, you can receive, by fax, marketing and technical information on many topics, including hardware, operating systems, and local area networks (LANs).

You can call the IBM Automated Fax System 24 hours a day, 7 days a week. Follow the recorded instructions, and the requested information will be sent to your fax machine. In the U.S. and Canada, to access the IBM Automated Fax System, call 1-800-426-3395.

---

### Getting help and service

If you have a problem with your server product, you will find a wide variety of sources available to help you.

### Using the documentation and diagnostic programs

Many problems can be solved without outside assistance. If you experience a problem with your server product, the first place to start is the troubleshooting information in your IBM documentation. If you suspect a software problem, see the documentation,

including README files and online help, that comes with the operating system or application program.

Most IBM server products come with a set of diagnostic programs that you can use to help you identify hardware problems. See the troubleshooting information in your IBM documentation for instructions on 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.

## Calling for service

If you have tried to correct the problem yourself and still need help, during the warranty period, you can get help and information by telephone through the IBM HelpCenter®. The following services are available during the warranty period:

- **Problem determination** - Trained personnel are available to assist you with determining if you have a hardware problem and deciding what action is necessary to fix the problem.
- **IBM hardware repair** - If the problem is determined to be caused by IBM hardware under warranty, trained service personnel are available to provide the applicable level of service.
- **Engineering Change management** - Occasionally, there might be changes that are required after a product has been sold. IBM or your reseller, if authorized by IBM, will make selected Engineering Changes (ECs) available that apply to your hardware.

The following items are not covered:

- Replacement or use of non-IBM parts or nonwarranted IBM parts. All warranted parts contain a 7-character identification in the format IBM FRU XXXXXXX.
- Identification of software problem sources.
- Configuration of BIOS as part of an installation or upgrade.
- Changes, modifications, or upgrades to device drivers.
- Installation and maintenance of network operating systems (NOS).
- Installation and maintenance of application programs.

Refer to your IBM Statement of Limited Warranty for a full explanation of IBM warranty terms. Be sure to retain your proof of purchase to obtain warranty service.

In the U.S. and Canada, these services are available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9:00 a.m. to 6:00 p.m.

**Note:** Response times vary; may exclude some holidays.

In addition, you are eligible for IBM Start Up Support for 90 days after installation. This service provides assistance for:

- Setting up your network operating system
- Installing and configuring interface adapters
- Installing and configuring network adapters

Please have the following information ready when you call:

- Machine type and model
- Serial numbers of your IBM hardware products
- Description of the problem

- Exact wording of any error messages
- Hardware and software configuration information

## Telephone numbers

Phone numbers are subject to change without notice. For the most up-to-date phone numbers, go to <http://www.ibm.com/pc/support/> and click **Support Phone List**.

| Country                |                         | Telephone number |
|------------------------|-------------------------|------------------|
| Austria                | Österreich              | 01-24 592 5901   |
| Belgium - Dutch        | Belgie                  | 02-210 9820      |
| Belgium - French       | Belgique                | 02-210 9800      |
| Canada                 | Toronto only            | 416-383-3344     |
| Canada                 | Canada - all other      | 1-800-565-3344   |
| Denmark                | Danmark                 | 45 20 82 00      |
| Finland                | Suomi                   | 09-22 931 840    |
| France                 | France                  | 02 38 55 74 50   |
| Germany                | Deutschland             | 07032-1549 201   |
| Ireland                | Ireland                 | 01-815 9202      |
| Italy                  | Italia                  | 02-7031 6101     |
| Luxembourg             | Luxembourg              | 298-977 5063     |
| Netherlands            | Nederland               | 020-514 5770     |
| Norway                 | Norge                   | 23 05 32 40      |
| Portugal               | Portugal                | 21-791 51 47     |
| Spain                  | España                  | 91-662 49 16     |
| Sweden                 | Sverige                 | 08-477 4420      |
| Switzerland            | Schweiz/Suisse/Svizzera | 058-333 0900     |
| United Kingdom         | United Kingdom          | 01475-555 055    |
| U.S.A. and Puerto Rico | U.S.A. and Puerto Rico  | 1-800-772-2227   |

In all other countries or regions, contact your IBM reseller or IBM marketing representative.

---

## International Warranty Service

If you travel with your server product or relocate it to a country where your server machine type is sold and serviced by IBM or by IBM resellers who are authorized to perform warranty service, International Warranty Service is available for your server product.

Service methods and procedures vary by country, and some services might not be available in all countries. International Warranty Service is delivered through the method of service (such as depot, carry-in, or on-site service) that is provided in the servicing country. Service centers in certain countries might not be able to service all models of a particular machine type. In some countries, fees and restrictions might apply at the time of service.

To determine whether your server product is eligible for International Warranty Service and to view a list of the countries where service is available, go to <http://www.ibm.com/pc/support/>, and click **Warranty Lookup**. Eligible IBM server products are identified by their four-digit machine types. For more information about International Warranty Service, see Service Announcement 601-034 at <http://www.ibm.com/>. Click **Support & downloads**, click **Announcement letters**, and click **Announcements search**. In the **Search by letter number only** field, type 601-034, and click **Search**.

---

## Purchasing additional services

During and after the warranty period, you can purchase additional services, such as support for IBM and non-IBM hardware, operating systems, and application programs; network setup and configuration; upgraded or extended hardware repair services; and custom installations. Service availability and service name might vary by country or region.

For more information about these services, contact your IBM marketing representative.

---

## Appendix B. Notices

This publication 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 publication 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.

Some software may differ from its retail version (if available) and may not include all user manuals or all program functionality.

---

### Edition notice

**© COPYRIGHT INTERNATIONAL BUSINESS MACHINES CORPORATION, 2001.  
All rights reserved.**

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

---

## Trademarks

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

|                        |                             |
|------------------------|-----------------------------|
| Alert on LAN           | Predictive Failure Analysis |
| Chipkill               | ServeRAID                   |
| EtherJet               | ServerGuide                 |
| e-business logo        | ServerProven                |
| HelpCenter             | TechConnect                 |
| HelpWare               | Tivoli                      |
| IBM                    | Tivoli Enterprise           |
| Light Path Diagnostics | Update Connector            |
| NetBAY                 | Wake on LAN                 |
| NetView                | xSeries                     |
| OS/2 WARP              |                             |

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

Intel, Celeron, MMX, LANDesk, Pentium, Pentium II Xeon, Pentium III Xeon, and Xeon 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.

Linux is a registered trademark of Linus Torvalds.

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

# Index

## A

- ASM
  - date setting 29
  - Ethernet connection, configuration 42, 72
  - remote control 17
  - restarting 51
  - time setting 29
- ASM interconnect network
  - accessing remote adapters 21
- ASM interconnect network, accessing remote adapters 86
- ASM interface
  - features 4
    - access remote 5
    - alerts 5
    - event log 4
    - log in profiles 5
    - log off 6
    - network interfaces 5
    - network protocols 6
    - power/restart 4
    - remote control 5
    - restart ASM 6
    - restore defaults 6
    - serial port 5
    - system 5
    - system health 4
    - vital product data 4
  - opening 3
  - using 3
- automatic daylight savings time update 29

## C

- changing the host server startup sequence 20
- configuration
  - backups 49
  - restoration of ASM 50
  - restoration of changed 50
- configuring remote control keys 38, 88
- configuring SMTP 49, 79
- configuring SNMP 47
- critical events 8

## D

- delay between retries, setting 35

## E

- event log
  - viewing 10, 82
    - component activity log 13
    - component level VPD 11

- error 10
- informational 10
- machine level VPD 11
- POST/BIOS data 12
- system data 12
- warning 10

## F

- factory defaults, restoring 88
- firmware, updating 21

## G

- GMToffset 29

## H

- host server startup sequence, changing 20

## I

- initialization-string guidelines 42, 72

## L

- local events
  - setting 37
- logging off 51, 89
- login profile
  - read-only 31
  - read/write 31
- login profiles
  - creating 61

## N

- notices and statements 2

## P

- power 8
- power-off delay 60
- PPP access
  - serial port, configuration 45
- PXE Boot Agent 20

## R

- remote alert
  - settings, warning alerts 36
- remote alert attempts
  - setting 66
- remote alert attempts, setting 34
- remote alert recipients
  - configuring 63
- remote alert retry limit, setting 35
- remote alerts
  - setting, critical alerts 35
- remote alerts, setting 35, 67
- remote control server power
  - O/S shutdown 16
  - power off server immediately 16
  - power on server immediately 16
  - restart server immediately 16
- remote POST, viewing 87
- remote servers
  - monitoring 8
    - temperature 8
    - thresholds 9
    - voltage 9
- Remote Supervisor Adapter
  - clock setting 80
  - login profiles
    - creating 30
  - server timeouts, setting 26
  - system information, setting 26
  - tasks 15
- Remote Supervisor Adapter features 1

## S

- serial port
  - configuring 70
- serial port access, configuring 75
- serial port, configuring 39
- server blue screen 18
- server graphical console 17
- server POST 18
- server power status
  - remotely controlling 86
- server timeouts
  - setting 58
- service summary 91
- settings
  - dial-in 31, 63
  - modem 31, 63
- SMTP configuration 49, 79
- SNMP, configuring 47, 77
- special keys, configuring 38, 88
- startup sequence, changing 20
- state 8
- system alerts 36
- system information, setting 57

## T

- terminal settings 54
- text-based interface
  - accessing using TELNET 53
  - accessing via a direct serial connection 54
  - configuring for Remote Supervisor Adapter 57
  - monitoring
    - fans 81
    - voltage 81
- trademarks 96

## U

- updating firmware 21

## V

- vital product data
  - viewing 11, 83

## W

- watchdog
  - loader 59
  - o/s 60
  - post 59
- Web browser requirements 2





Part Number: 33P2677  
File Number:



Printed in the United States of America  
on recycled paper containing 10%  
recovered post-consumer fiber.

33P2677

