



Remote Supervisor Adapter User's Guide

for the IBM [®]@server xSeries 330



Remote Supervisor Adapter



User's Guide for the xSeries 330

Note: Before using this information and the product it supports, be sure to read the general information in Appendix B, "Notices," on page 97.

Fifth Edition (September 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

Chapter 1. Introduction	1
Remote Supervisor Adapter features	1
Web browser requirements	2
Notices used in this book	2
Chapter 2. Logging into and using the ASM Web interface	3
Logging into the Remote Supervisor Adapter	3
Logging into the ASM processor	6
Chapter 3. Monitoring system health	9
Monitoring remote server system health	9
Viewing the event log	13
Viewing the Remote Supervisor Adapter event log	13
Viewing the ASM processor event log	14
Viewing vital product data	14
Viewing VPD for the Remote Supervisor Adapter	14
Viewing VPD for the ASM processor and remote managed server	15
Chapter 4. Performing Remote Supervisor Adapter tasks	17
Updating firmware	17
Updating Remote Supervisor Adapter firmware	17
Updating firmware when logged into the ASM processor	18
Accessing remote adapters through ASM interconnect network	18
Server power and restart activity	20
Remotely controlling the power status of a server	21
Chapter 5. Configuring your Remote Supervisor Adapter and ASM processor.	
23	
Setting system information	24
Setting server timeouts	25
Setting the date and time	27
Creating login profiles	28
Creating a login profile on the Remote Supervisor Adapter	28
Creating a login profile on the ASM processor	30
Setting the modem and dial-in settings	31
Configuring remote alert settings	32
Setting remote alert attempts	34
Setting remote alerts	35
Setting local events	37
Configuring the serial ports	37
Initialization-string guidelines	40
Configuring network interfaces	40
Configuring an Ethernet connection to Remote Supervisor Adapter	40
Configuring PPP access over a serial port	43
Configuring network protocols	45
Configuring SNMP	45
Configuring DNS	46
Configuring SMTP	47
Using the configuration file	48
Backing up your current Remote Supervisor Adapter configuration	48
Restoring your ASM configuration	49
Restoring ASM defaults	49
Restarting ASM	49
Logging off	50

Chapter 6. Starting and configuring the ASM text-based interface	51
Accessing a text-based interface via a TELNET connection	51
Accessing remote adapters through an ASM interconnect network.	52
Accessing a text-based interface via a direct serial connection	52
Configuring terminal settings	53
Chapter 7. Configuring your Remote Supervisor Adapter or ASM processor using a text-based interface	55
Setting system information	56
Setting Remote Supervisor Adapter system information	56
Setting Remote Supervisor Adapter system information	57
Setting server timeouts.	58
Creating login profiles.	60
Creating a login profile on the Remote Supervisor Adapter.	60
Creating a login profile on the ASM processor.	62
Setting modem and dial-in settings	64
Configuring remote alert recipients	65
Setting remote alert attempts	67
Setting remote alerts	68
Configuring the serial port	71
Configuring the serial port in the Remote Supervisor Adapter	71
Configuring the serial ports in the ASM processor.	73
Initialization-string guidelines	75
Configuring network interfaces.	75
Configuring an Ethernet connection to the Remote Supervisor Adapter	75
Configuring PPP access over a serial port.	78
Configuring network protocols	80
Configuring SNMP	80
Configuring DNS	81
Configuring SMTP	82
Setting the date and time	82
Setting the date and time on the Remote Supervisor Adapter.	82
Setting the date and time on the ASM processor.	83
Chapter 8. Text-based interface system health and tasks	85
Monitoring temperatures, voltage, and fan readings	85
Viewing the event log	86
Viewing the Remote Supervisor Adapter event log	86
Viewing the ASM processor event log	87
Viewing vital product data	88
Viewing VPD for the Remote Supervisor Adapter	88
Viewing VPD for the ASM processor	88
Performing Remote Supervisor Adapter tasks through a text-based interface.	90
Accessing remote adapters through ASM interconnect network	90
Powering on or restarting servers	91
Viewing server text console	91
Restoring ASM to factory defaults	91
Restarting ASM	91
Logging off	91
Appendix A. Getting help, information and service	93
Getting information	93
Using the World Wide Web	93
Getting information by fax	93
Getting help and service.	93
Using the documentation and diagnostic programs	93

Calling for service	94
Telephone numbers	95
Purchasing additional services	95
Appendix B. Notices	97
Edition notice	97
Trademarks	98
Important notes	98

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 330. 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 the 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
- Remote firmware update
- Access to critical server settings
- Text-based user interface terminal access

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:

- **Notes:** These notices provide important tips, guidance, or advice.
- **Important:** These notices provide information or advice that might help you avoid inconvenient or problem situations.
- **Attention:** These notices indicate 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. Logging into and using the ASM Web interface

Certain features of the ASM Web interface and text-based interface are available only through the ASM processor that is integrated on the system board of your server. You must first log into the Remote Supervisor Adapter and then log into the ASM processor to access these features. This chapter describes the login procedures and the features and functions of the Remote Supervisor Adapter or the ASM processor.

Logging into the Remote Supervisor Adapter

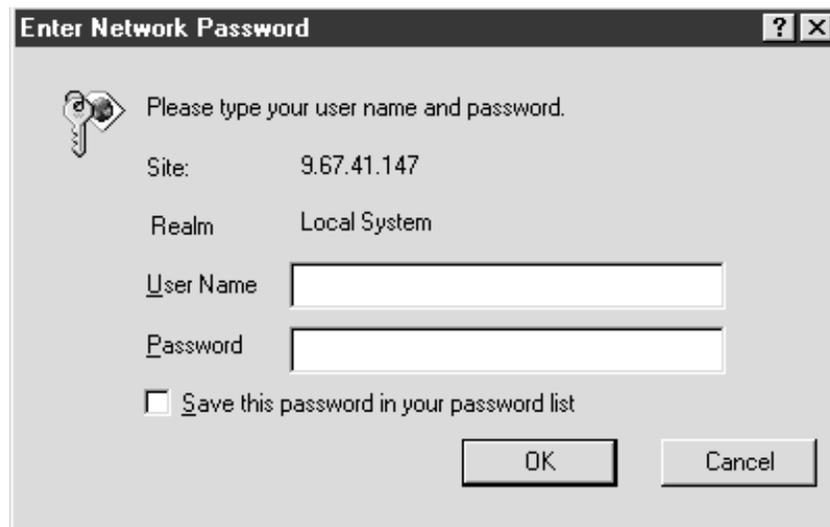
This section explains the features that are accessible when you are logged into only the Remote Supervisor Adapter. When you are logged into the Remote Supervisor Adapter and then log into the ASM processor integrated on the server system board, some of these features are enhanced.

To log into the Remote Supervisor Adapter using the ASM Web interface, complete the following steps:

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

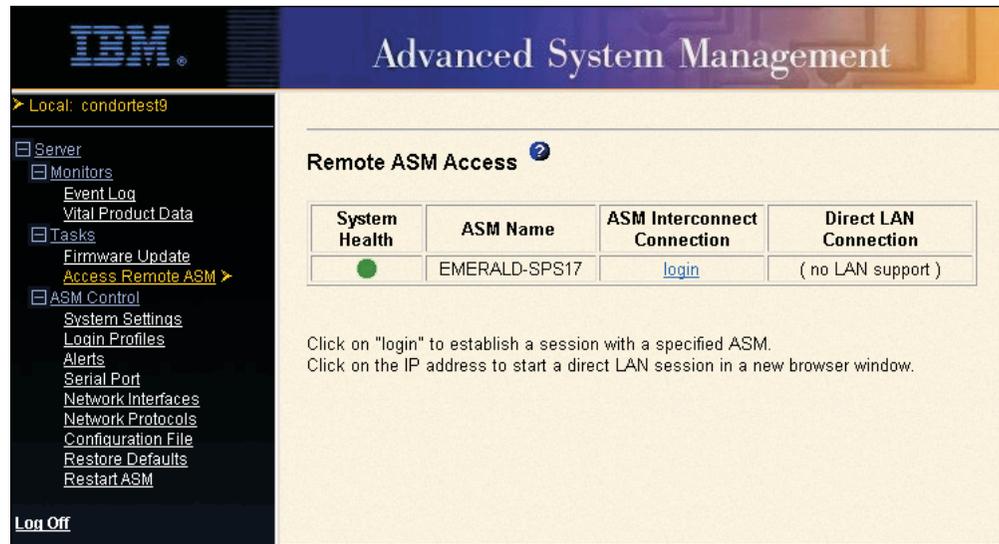
OK Cancel

2. In the Enter Network Password screen, type your user name and password. 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 (the 0 is a zero). 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 the number of minutes you select, the Remote Supervisor Adapter logs you off the Web interface.

- Click **Continue** to start the session. The browser opens the Remote ASM Access home page.



You are now logged into the Remote Supervisor Adapter. The following table lists the features you have access to through the links provided on the navigation frame.

Note: When you are logged into a Remote Supervisor Adapter or an ASM processor, the link names used by the Web interface are identical; however, the information and functions that are supported differ. In the following table, these features are explained as they function when you are logged into the Remote Supervisor Adapter.

Table 1. Actions available when logged into the Remote Supervisor Adapter.

Link	Action	Description
System Settings	Configure the system settings	You can configure information about the Remote Supervisor Adapter, such as the name, contact, and location information on the System Settings page.
Event Log	View the event log for Remote Supervisor Adapter events	The event log page contains information specific to the Remote Supervisor Adapter, such as remote access attempts and dial-out events. All events in the log are time-stamped using the Remote Supervisor Adapter clock.
Vital Product Data	View the Remote Supervisor Adapter vital product data (VPD)	You can view information about the Remote Supervisor Adapter application and boot ROM firmware data from the Vital Product Data page.
Firmware Update	Update the Remote Supervisor Adapter firmware	You can update the firmware of the Remote Supervisor Adapter from the Firmware Update page.
Access Remote ASM	Establish an ASM interconnect connection to the server on the network	You can view a list of the ASM processors, ASM PCI adapters, and Remote Supervisor Adapters present on the ASM interconnect network and establish a connection to any of those systems. Use this page to log into the ASM processor within a given server.
Alerts	Configure alert forwarding	The Remote Supervisor Adapter forwards alerts generated by the ASM processor. It does not generate alerts on its own. You can configure settings for forwarding alerts from the Alerts page.

Table 1. Actions available when logged into the Remote Supervisor Adapter.

Link	Action	Description
Serial Port	Configure the serial port of a Remote Supervisor Adapter	You can configure the serial port and modem settings used by the Remote Supervisor Adapter from the Serial Port page. Note: The serial port used by the Remote Supervisor Adapter is different from the serial port used by the ASM processor. The Remote Supervisor Adapter has a dedicated serial port.
System Settings	Set the Remote Supervisor Adapter clock	You can set the clock used by the Remote Supervisor Adapter for time-stamping the entries in the event log.
Login Profiles	Configure login profiles on the Remote Supervisor Adapter	You can define up to twelve login profiles that enable access to the Remote Supervisor Adapter from the Login Profiles page.
Network Interfaces	Configure the network interfaces of the Remote Supervisor Adapter	You can configure network-access settings to the Remote Supervisor Adapter from the Network Interfaces page, which is only available when you log into the Remote Supervisor Adapter. The Remote Supervisor Adapter supports both Ethernet and point-to-point protocol (PPP) connections, enabling remote access using a Web browser or TELNET application.
Network Protocols	Configure the network protocols of the Remote Supervisor Adapter	You can configure Simple Network Management Protocol (SNMP), Domain Name System (DNS), and Simple Mail Transfer Protocol (SMTP) settings used by the Remote Supervisor Adapter from the Network Protocols page, which is only available when you log into the Remote Supervisor Adapter.
Configuration File	Backup and restore the Remote Supervisor Adapter configuration	You can backup, modify, and restore the configuration of the Remote Supervisor Adapter from the Configuration File page.
Restore Defaults and Restart ASM	Restore and restart the Remote Supervisor Adapter defaults	You can reset the Remote Supervisor Adapter configuration to the factory defaults from the Restore Defaults page. You can restart the Remote Supervisor Adapter from the Restart ASM page.
Log Off	Log off the Remote Supervisor Adapter	You can log off from the Remote Supervisor Adapter from the Log Off page.

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

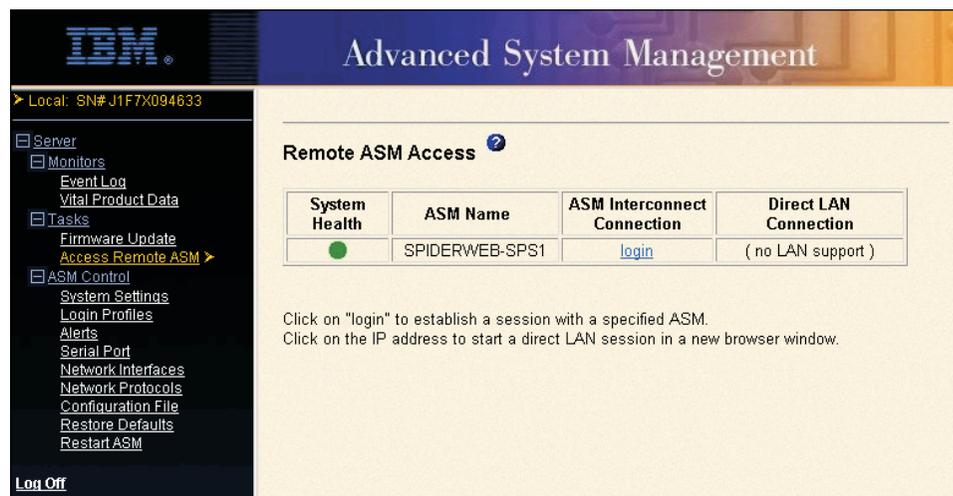
Logging into the ASM processor

When you initially log into the ASM Web interface of the Remote Supervisor Adapter, you can view a list of the ASM processors, ASM adapters, and Remote Supervisor Adapters in the interconnect network and the local system that contains the Remote Supervisor Adapter.

The integrated ASM processor in the xSeries 330 enables you to monitor managed server's health, view the server event log and vital product data, configure alerts and alert recipients, and perform power and restart operations on the server.

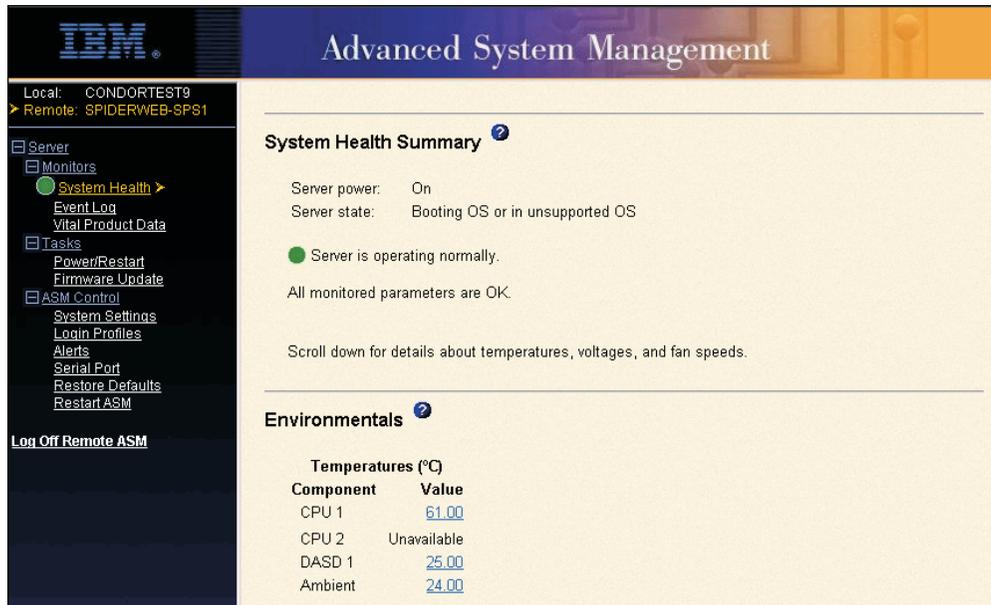
To log into an ASM processor through the Remote Supervisor adapter, do the following:

1. Log into the Remote Supervisor Adapter through the ASM Web interface. See "Logging into the Remote Supervisor Adapter" on page 3.
2. In the navigation frame, click **Access Remote ASM**. The Remote ASM Access page opens.



System Health	ASM Name	ASM Interconnect Connection	Direct LAN Connection
	SPIDERWEB-SPS1	login	(no LAN support)

3. In the ASM Interconnect Connection column for the entry that matches the ASM processor of the server that you want to monitor, click **login**.
Note: It is important that you name the ASM processor of each server with meaningful names so that you can easily identify the correct server to monitor. The name of the processor is what you select from the table in the ASM Interconnect column. If you are not sure of the name of the ASM processor for the server that you want to monitor, log into each ASM processor individually and view the vital product data (VPD) to determine the serial number of the server in which that ASM processor is located.
4. Log into the remote ASM processor. The System Health page for the monitored server is displayed.



The following table lists the features as they function when you are logged into the ASM processor. After you log into the ASM processor, you have access to the following features:

Table 2. Actions available when logged into the ASM processor.

Link	Action	Description
System Settings	View the ASM processor system settings	You can configure general information such as the name of the ASM processor, ID number, and server time-out settings from the System Settings page.
System Health	View system health for the ASM processor	You can monitor the power and restart, temperature, voltage, and fan status of your server on the System Health page.
Event Log	View event logs for remote servers	The event log page contains entries that are stored in the system event and POST event logs. Information about all remote access attempts and dial-out events are recorded in the event log. All events in the log are time-stamped using the ASM processor date and time settings. Some events will also generate an alert, if configured to do so on the alerts page.
Vital Product Data	View the server and ASM processor VPD	Upon server startup, the ASM processor collects system and basic input/output system (BIOS) code, and server component vital product data (VPD) and stores it in nonvolatile memory. This data is available from the Vital Product Data page.
System Settings	Set the ASM processor clock	You can set the clock used by the ASM processor for timestamping the entries in the event log.
Login Profiles	Configure the ASM processor login profiles	You can define twelve login profiles that enable access to the ASM processor. For more information on defining login profiles, see “Creating login profiles” on page 28.
Alerts	Configure local events	You can set the local events monitored by the ASM processor, for which notifications are sent to the IBM Director.

Table 2. Actions available when logged into the ASM processor.

Link	Action	Description
Power/Restart	Remotely power on or restart a server	The ASM processor 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. These features are accessed from the Power/Restart page, which is only available when you log onto the ASM processor.
Firmware Update	Update firmware on a server or the ASM processor	Use the options on the Firmware Update page to update firmware of the ASM processor and server components such as server BIOS code and server diagnostics.
Alerts	Configure remote alerts and remote alert recipients	You can configure the ASM processor to generate and forward alerts for a number of different events. You can configure the alerts that are monitored and the recipients that are notified on the Alerts page. For more information on configuring remote alert recipients and the alerts to send, see "Setting remote alert attempts" on page 34.
Alerts	Configure alert settings	You can set the number of alert retries and the delay between the retries.
Serial Port	Dedicate a serial port to an ASM processor or share access with a host server	You can configure the serial port and modem settings used by the ASM processor from the Serial Port page. For more information on the serial port, see "Configuring the serial ports" on page 37. Note: The serial port used by the ASM processor is different from the serial port provided on the Remote Supervisor Adapter. The ASM processor uses the serial port of the server. One of those serial ports can either be shared with the operating system running on the server or it can be dedicated to the ASM processor. The other port is always dedicated to the ASM processor.
Restore Defaults	Restore the ASM processor defaults	Attention: When you click Restore Defaults, all of the modifications you made to the ASM processor are lost. You can reset the configuration of the ASM processor to the factory defaults here. For more information on restoring defaults, see "Restoring ASM defaults" on page 49.
Restart ASM	Restart an ASM processor	You can restart the ASM processor. For more information on restarting, see "Restarting ASM" on page 49.
Log Off Remote ASM	Log off a remote ASM processor	This link logs off your connection to the ASM processor and returns to the Remote Supervisor Adapter that originated the remote session. For more information on logging off, see "Logging off" on page 50.

You can click the **View Configuration Summary** link, which appears on most pages, to quickly view the configuration of the ASM processor.

Chapter 3. Monitoring system health

Use the links under the Monitors heading of the navigation frame to view the status of the server you access. The monitoring features available to you depend on whether you are logged into the Remote Supervisor Adapter or the ASM processor.

When logged into the Remote Supervisor Adapter, you can:

- View the Remote Supervisor Adapter event log
- View vital product data (VPD) of the Remote Supervisor Adapter main application and boot ROM firmware

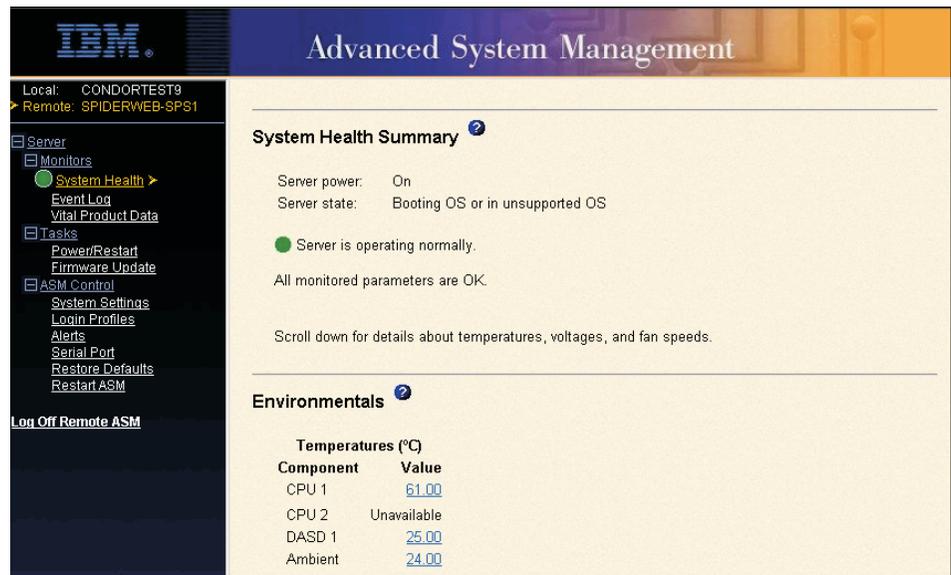
When logged into the ASM processor, you can:

- View the system health and environmental readings of the remote server
- View the event log of the ASM processor and the remote managed server
- View the VPD of the ASM processor and the remote managed server

Monitoring remote server system health

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

1. Log into the Remote Supervisor Adapter. For more information, see “Logging into the Remote Supervisor Adapter” on page 3.
 2. Log into the ASM processor. See “Logging into the ASM processor” on page 6.
- A System Health Summary window similar to the following opens:



The screenshot shows the IBM Advanced System Management (ASM) web interface. The navigation frame on the left includes links for Server, Monitors, System Health (selected), Event Log, Vital Product Data, Tasks, Power/Restart, Firmware Update, ASM Control, System Settings, Login Profiles, Alerts, Serial Port, Restore Defaults, Restart ASM, and Log Off Remote ASM. The main content area displays the System Health Summary page, which includes the following information:

- System Health Summary**
- Server power: On
- Server state: Booting OS or in unsupported OS
- Server is operating normally.
- All monitored parameters are OK.
- Scroll down for details about temperatures, voltages, and fan speeds.
- Environmentals**
- Temperatures (°C)
- Component Value
- CPU 1 61.00
- CPU 2 Unavailable
- DASD 1 25.00
- Ambient 24.00

In the navigation frame, you can click **System Health** to view a dynamically-generated update on the overall health of the server.

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. View the `Server Power/Restart Activity` section, which gives the current power status of the system.

Server power

Indicates the power status of the server.

Server state

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

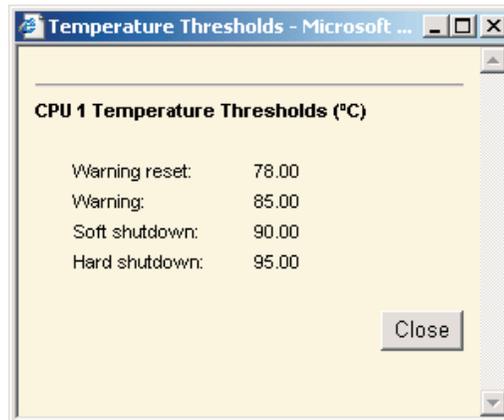
- `System power off/State unknown`
 - `In POST`
 - `Stopped in POST (Error detected)`
 - `Booted Flash or System partition`
 - `Booting OS or in OS (Could be in the OS if the OS or application does not report the new system state.)`
 - `In OS`
 - `CPU's held in reset`
4. Scroll down to the `Environmentals` section. The `Remote Supervisor Adapter` tracks the current temperature readings and threshold levels for system components such as microprocessors, system boards, and hard disk drive backplanes.

Temperatures (°C)	
Component	Value
CPU 1	52.00
CPU 2	Unavailable
DASD 1	25.00
Ambient	24.00

Voltages (v)	
Source	Value
+5v	+5.09
+3v	+3.33
+12v	+11.98
+2.5v	+2.67
VRM 1	+ 1.74
VRM 2	+ 1.36

Fan Speeds (% of max)	
Fan	Speed
1	75%
2	74%
3	74%
4	76%
5	75%
6	76%

5. When you click a temperature reading, a window similar to the following opens:



The Temperature Thresholds window displays the temperature levels at which the ASM processor 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 ASM processor 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** check box 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

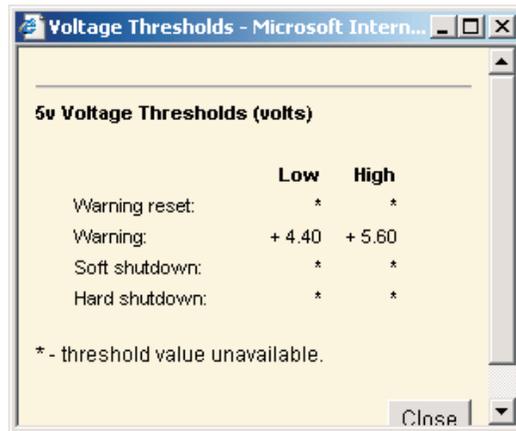
When the temperature reaches a specified value higher than the warning value (the soft shutdown threshold), a second temperature warning is sent to remote alert recipients and the server begins the shutdown process with an orderly operating system shutdown. The server then turns itself off. You must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

6. Scroll down to the Voltages section. The ASM processor will send an alert if the monitored power source voltage falls outside its specified operational range.

When you click a voltage reading, a window similar to the following opens:



The Voltage Thresholds window displays the voltage ranges at which the ASM processor 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 regulation 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 ASM processor 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** check box 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** check box 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** check box on the Alerts page for the warning to be sent.

7. 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 check boxes 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 or processor event log. The ASM processor 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

Note: You need to log into the ASM processor to view the system error log and POST error log.

Viewing the Remote Supervisor Adapter event log

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 "Logging into the Remote Supervisor Adapter" on page 3.
2. In the navigation frame, click **Event Log** to view the history of Remote Supervisor Adapter and ASM processor logins. The event log also displays Remote Supervisor Adapter-specific data, such as:
 - Resets and bootups
 - Interconnect connections
 - Firmware updates
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.

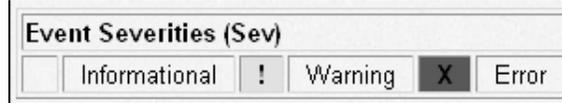
Warning

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 the ASM processor event log

The event log has a limited capacity. When that limit is reached, the older events are deleted in a first-in, first-out order. You can select 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 “Logging into the Remote Supervisor Adapter” on page 3.
2. Log into the ASM processor. For more information, see “Logging into the ASM processor” on page 6.
3. In the navigation frame, click **Event Log** to view the recent history of events on the server.
4. 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 ASM processor collects system and basic input/output (BIOS) vital product data, and stores it in nonvolatile memory. The Vital Product Data page contains key information about the system that the Remote Supervisor Adapter is monitoring.

Viewing VPD for the Remote Supervisor Adapter

Complete the following steps to view the VPD for the Remote Supervisor Adapter application and the boot ROM firmware.

1. Log into the Remote Supervisor Adapter. For more information, see “Logging into the Remote Supervisor Adapter” on page 3.
2. In the navigation frame, click **Vital Product Data**.
The ASM VPD window appears.

ASM VPD				
Firmware Type	Build ID	Revision	File Name	Release Date
Main Application	FBET04+	16	CNETMNUS.PKT	07-11-01
Boot ROM	FBBR04+	16	CNETBRUS.PKT	07-11-01

You can check the ASM VPD window for the level of the firmware used by the Remote Supervisor Adapter.

Viewing VPD for the ASM processor and remote managed server

Complete the following steps to view the monitored ASM processor.

1. Log into the Remote Supervisor Adapter. For more information, see “Logging into the Remote Supervisor Adapter” on page 3.
2. Log into the ASM processor. For more information, see “Logging into the ASM processor” on page 6.
3. In the navigation frame, click **Vital Product Data**. You can view the following:

Machine level VPD

The VPD for the server appears in this section.

Note: The Machine level VPD will only provide information when the server is powered on.

Table 3. Machine level vital product data.

Field	Function
Machine type	Identifies the type of server the ASM processor is monitoring.
Machine model	Identifies the model number of the server the ASM processor is monitoring.
Serial number	Identifies the serial number of the server the ASM processor is monitoring.

POST/BIOS data

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

Table 4. 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.

ASM processor system data

You can find the VPD for the ASM processor in this section.

Table 5. Remote Supervisor Adapter vital product data.

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

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. While logged into the Remote Supervisor Adapter, you can perform the following tasks:

- Update Remote Supervisor Adapter firmware
- Access other Remote Supervisor Adapters

While logged into the ASM processor, you can perform the following tasks:

- Update ASM processor firmware
- Power up or restart the server

Updating firmware

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

Updating Remote Supervisor Adapter firmware

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

1. Log into the Remote Supervisor Adapter. For more information, see “Logging into the Remote Supervisor Adapter” 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.
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 whether 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** until you return to the Transfer Files page.

Updating firmware when logged into the ASM processor

Complete the following steps to update the ASM processor firmware, or the server firmware components such as BIOS or diagnostics.

1. Log into the Remote Supervisor Adapter. For more information, see “Logging into the Remote Supervisor Adapter” on page 3.
2. Log into the ASM processor. For more information, see “Logging into the ASM processor” on page 6.
3. In the navigation frame, click **Firmware Update**.
4. Click **Browse**.
5. Navigate to the PKT or PKC file you want to update.
6. Click **Open**.

The file (including the full path) appears in the box beside **Browse**.

7. 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.

8. 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.
9. To complete the update process, click **Continue**.

A progress indicator opens as the firmware on the ASM processor is flashed. A confirmation page opens to verify that the update was successful.

10. After receiving a confirmation that the update process is complete, go to the Restart ASM page and click **Restart**.
11. Click **OK** to confirm that you want to restart the Remote Supervisor Adapter.
12. Click **OK** to close the current browser window.
13. 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** until you return to the Transfer Files page.

Accessing remote adapters through 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 an ASM processor, ASM PCI adapter, or Remote Supervisor Adapter on the ASM interconnect network:

1. Log into the Remote Supervisor Adapter. For more information, see “Logging into the Remote Supervisor Adapter” 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.

Remote ASM Access 			
System Health	ASM Name	ASM Interconnect Connection	Direct LAN Connection
	SPS17	login	(no LAN support)

Click on "login" to establish a session with a specified ASM.
Click on the IP address to start a direct LAN session in a new browser window.

The table displays the following information:

System Health

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

ASM Name

The name of the remote ASM processor 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 logon to a remote system displayed in the table, click the login link corresponding to the remote system that you want to access. Then follow the standard login procedure to gain access to that system.

Direct LAN Connection

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

To logon directly to 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 one of the following:

no LAN support

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

function not supported

The systems-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 systems-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

3. Click the **login** link that corresponds to the processors and adapters that you want to access under the ASM 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 ASM processor and Remote Supervisor Adapter names appear in orange above the navigation frame.

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

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 ASM 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 IBM System Management 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.

Chapter 5. Configuring your Remote Supervisor Adapter and ASM processor

Use the links under the ASM Control heading in the navigation frame to configure your Remote Supervisor Adapter. The monitoring features available to you depend on whether you are logged into the Remote Supervisor Adapter or the ASM processor.

- From the System page, you can:
 - Set system information
 - Set server timeouts
 - Set ASM processor date and time
- From the Login Profiles page, you can:
 - Set login profiles to control access to the Remote Supervisor Adapter
 - 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 of the Remote Supervisor Adapter
 - 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 Restart ASM page, you can restart the Remote Supervisor Adapter.

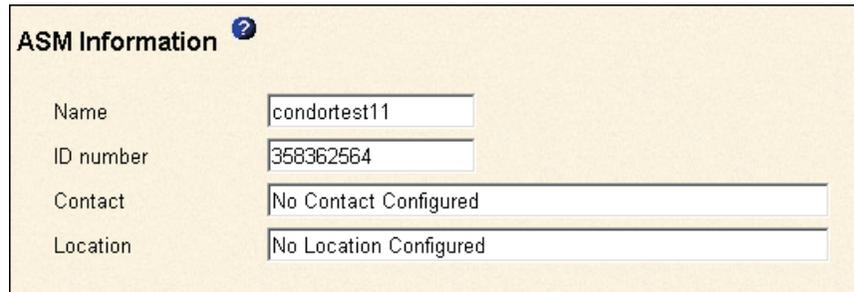
Setting system information

Complete the following steps to set your system information:

1. Log into the Remote Supervisor Adapter. For more information, see “Logging into the Remote Supervisor Adapter” on page 3.

To set the system information on the ASM processor, log into the ASM processor. For more information, see “Logging into the ASM processor” on page 6.

2. In the navigation frame, click **System Settings**. A window similar to the following opens:



The screenshot shows a web interface 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 or the ASM processor. 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 IP host name of the Remote Supervisor Adapter (the Hostname field on the Network Interfaces page) do not automatically share the same name because the Name field is limited to 15 characters. The Hostname field can consist of up to 63 characters. To minimize confusion, set the 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 Remote Supervisor Adapter” on page 40.

4. In the ID Number field, assign the Remote Supervisor Adapter or ASM processor a unique identification number.
5. In the Contact field, type the contact information. For example, you can specify the name and phone number of the person to contact if there is a problem with this server. You can type a maximum of 47 characters in this field.

Note: This field only appears when you are logged into the Remote Supervisor Adapter.

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.

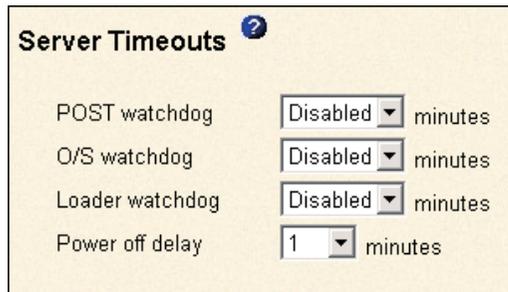
Note: This field only appears when you are logged into the Remote Supervisor Adapter.

Setting server timeouts

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

1. Log into the Remote Supervisor Adapter. For more information, see “Logging into the Remote Supervisor Adapter” on page 3.
2. Log into the ASM processor. For more information, see “Logging into the ASM processor” on page 6.
3. In the navigation frame, click **System Settings**, and scroll down to the Server Timeouts section.

A window similar to the following opens:



Server Timeouts ?	
POST watchdog	Disabled minutes
O/S watchdog	Disabled minutes
Loader watchdog	Disabled minutes
Power off delay	1 minutes

You can set the ASM processor to respond automatically to these events:

- Halted power-on self-test
 - Halted operating system
 - Failure to load operating system
 - Power off delay to shut down operating system
4. Enable the server timeouts that correspond to the events you want the ASM processor to respond to automatically.

POST watchdog

Use the POST watchdog field to specify the number of minutes that the ASM processor 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 ASM processor 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 ASM processor 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 ASM processor. If the operating system fails to

respond to one of these checks, the ASM processor 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 ASM processor 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 ASM processor 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 ASM processor waits between the completion of POST and the loading of the operating system. If this interval is exceeded, the ASM processor 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 ASM processor 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 ASM processor will send an alert to all enabled remote alert recipients.

Power off delay

Use the Power off delay field to specify how long the ASM processor 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 both the IBM Director with UM Server Extensions agent code and the ASM processor device driver 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 ASM processor, see the *UM Server Extensions User's Guide*.

Setting the date and time

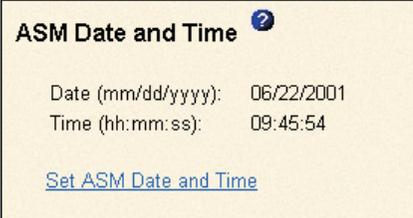
The Remote Supervisor Adapter and ASM processor contain internal clocks. Setting one does not affect the settings on the other, and each serve separate purposes.

Setting the date and time on the Remote Supervisor Adapter

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 sent alerts. 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.

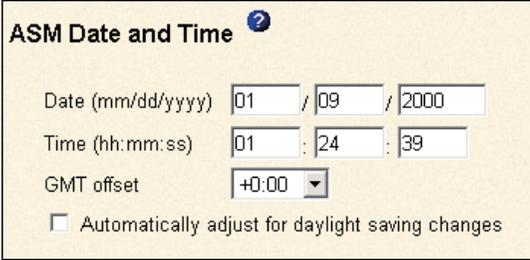
Complete the following steps to check the settings of the date and time on the Remote Supervisor Adapter.

1. Log into the Remote Supervisor Adapter. For more information, see “Logging into the Remote Supervisor Adapter” 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 opens:



The screenshot shows a window titled "ASM Date and Time" with a help icon. It displays the current date as 06/22/2001 and the current time as 09:45:54. Below the display is a blue link labeled "Set ASM Date and Time".

3. Click **Set ASM Date and Time**.



The screenshot shows the "ASM Date and Time" settings page with input fields. The Date field is set to 01 / 09 / 2000. The Time field is set to 01 : 24 : 39. The GMT offset is set to +0:00. There is a checkbox for "Automatically adjust for daylight saving changes" which is currently unchecked.

4. To set the Date field, type the numbers of the current month, day, and year in the matching text boxes.
5. 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.

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.

6. Click **Save**.

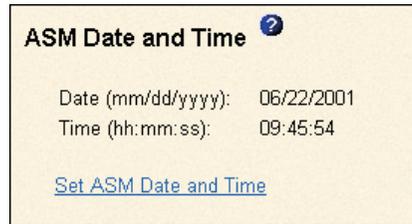
Setting the date and time on the ASM processor

The ASM processor 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 sent alerts. 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 settings on either the Remote Supervisor Adapter or the ASM processor

1. Log into the Remote Supervisor Adapter. For more information, see “Logging into the Remote Supervisor Adapter” on page 3.
2. Log into the ASM processor. For more information, see “Logging into the ASM processor” on page 6.
3. 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:



4. Click **Set ASM Date and Time**.
5. To set the Date, type the numbers of the current month, day, and year in the matching text boxes.
6. 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.
7. Click **Save**.

Creating login profiles

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

To change a login profile, click the link corresponding to that profile to open a page with profile setup details.

Note: By default, the ASM subsystem comes configured with one login profile that enables remote access using a login 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 ASM subsystem.

Creating a login profile on the Remote Supervisor Adapter

Complete the following steps to configure a login profile:

1. Log into the Remote Supervisor Adapter. For more information, see “Logging into the Remote Supervisor Adapter” 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 Profiles ?

To configure a login profile, click a link in the "Login ID" column.

Login ID	Access
1. USERID	Read/Write
2. H	Read/Write
3. ~ not used ~	
4. ~ not used ~	
5. ~ not used ~	
6. ~ not used ~	
7. ~ not used ~	
8. ~ not used ~	
9. ~ not used ~	
10. ~ not used ~	
11. ~ not used ~	
12. ~ not used ~	

Use this page to view, configure, or change individual login profiles. You can define up to twelve unique profiles.

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

Login Profile 1 ?

Login ID:

Authority level:

Password:

Confirm password:

Dialback status:

Dialback number:

- 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.

- 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. If you select **Disabled**, go to step 11 on page 31.
Note: If this menu is enabled, you must enter a phone number in the Dialback number field of this profile.
9. In the Dialback number field, type the phone number 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.
10. Click **Save** to save your login ID settings.

Creating a login profile on the ASM processor

Complete the following steps to configure a login profile:

1. Log into the Remote Supervisor Adapter. For more information, see “Logging into the Remote Supervisor Adapter” on page 3.
2. Log into the ASM processor. For more information, see “Logging into the ASM processor” on page 6.
3. 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. USERID	Read/Write
2. H	Read/Write
3. ~ not used ~	
4. ~ not used ~	
5. ~ not used ~	
6. ~ not used ~	
7. ~ not used ~	
8. ~ not used ~	
9. ~ not used ~	
10. ~ not used ~	
11. ~ not used ~	
12. ~ not used ~	

Use this page to view, configure, or change individual login profiles. You can define up to twelve unique profiles.

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

Login Profile 1 ?

Login ID: Jones

Authority level: Read/Write

Password: ****

Confirm password: ****

Dialback status: Disabled

Dialback number: [Empty field]

- 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 ASM processor.

- 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.

- 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.

- In the Confirm Password field, type the password again.
- 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. If you select **Disabled**, go to step 11.

Note: If this menu is enabled, you must enter a phone number in the Dialback number field of this profile.

- In the Dialback number field, type the phone number the Remote Supervisor Adapter to use when dialing-back to reach the login ID.
This phone number is dialed when the user defined in this profile successfully logs into the Remote Supervisor Adapter.
- Click **Save** to save your login ID settings.

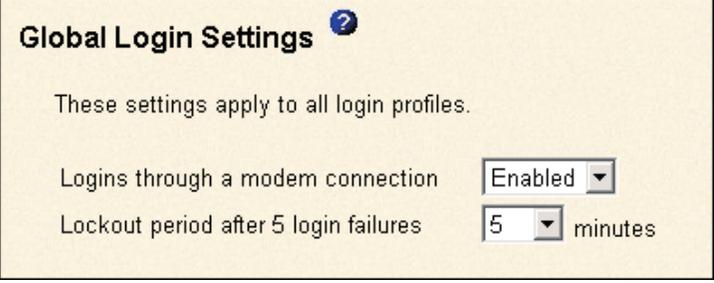
Setting the modem and dial-in settings

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

- Log into the Remote Supervisor Adapter. For more information, see “Logging into the Remote Supervisor Adapter” on page 3.

To set the modem and dial-in settings on the ASM processor, log into the ASM processor. For more information, see “Logging into the ASM processor” on page 6.

2. In the navigation frame, click **System Settings** and **Login Profiles**; then, scroll down to the Global Login Settings section.



Global Login Settings ?

These settings apply to all login profiles.

Logins through a modem connection

Lockout period after 5 login failures minutes

3. In the Logins through a modem connection field, select **Enabled** to enable remote users to dial into the ASM processor through a serial connection.
4. In the Lockout period after 5 login failures field, 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 settings

The ASM processor monitors the server and generates alerts in response to certain events. The Remote Supervisor Adapter cannot generate alerts; it can only forward the alerts generated by the ASM processor or other devices on the same ASM interconnect network. Alerts are sent only once per connection type. If one connection device fails, the alerts are forwarded to other devices on the same interconnect network.

You must log into the ASM processor to configure alert recipients, global alert settings, and incidents that trigger remote alerts and local events. Use the remote alert recipient links to view, configure, or change individual alert recipients. You can define up to twelve remote alert recipients. When logged into the Remote Supervisor Adapter, you can only configure settings for forwarding alerts such as the number of retries and the delay between retries.

After you configure a remote alert recipient, the ASM processor will send an alert to that recipient when any event selected from the Monitored 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.

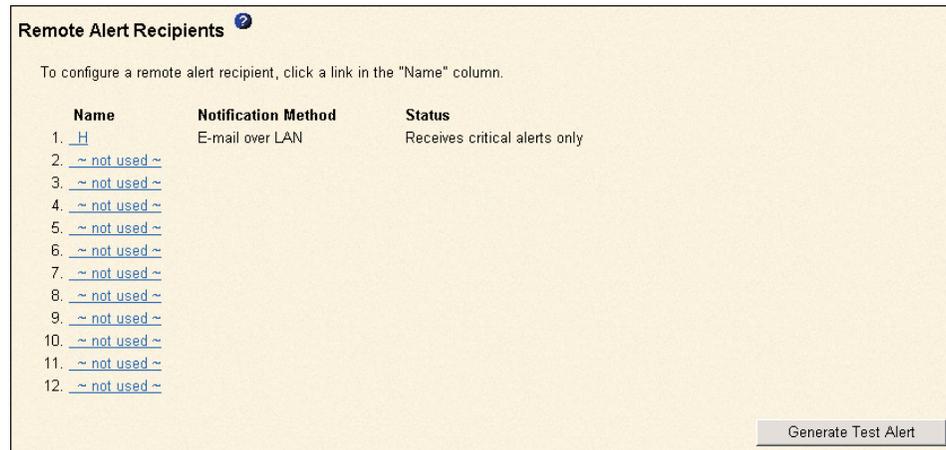
If the ASM processor cannot send out the alert itself, it forwards the alert to the Remote Supervisor Adapter. SNMP over LAN and IBM Director over LAN alerts are always forwarded by the ASM processor because it does not have LAN connectivity. For SNMP alerts, the configuration of the SNMP agent has to be done on the Remote Supervisor Adapter. For more information on these fields, see “Configuring SNMP” on page 45.

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 “Logging into the Remote Supervisor Adapter” on page 3.

- Log into the ASM processor. For more information, see “Logging into the ASM processor” on page 6.
- 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:



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

- In the Status field, click **Enabled**.
- 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.
- 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

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.

- 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 the personal identification number [PIN])
- Alphanumeric pager
- IBM Director over Modem

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

9. If you chose alphanumeric pager as the notification method, enter the PIN in the PIN field.
10. If you selected the SNMP over LAN method, configure the SNMP options on the Remote Supervisor Adapter Network Protocols page. Note that SNMP over LAN and IBM Director over LAN alerts are always forwarded because the ASM processor does not have LAN connectivity.
11. Click **Save** to save your remote alert recipient profile. Repeat steps 3 through 11 for each remote alert recipient profile.
12. 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 “Setting remote alerts” on page 35.

Setting remote alert attempts

When logged into the ASM processor, the remote alert attempts settings apply to the alerts generated by the ASM processor. When logged into the Remote Supervisor Adapter, these settings apply only to forwarded alerts.

1. Log into the Remote Supervisor Adapter. For more information, see “Logging into the Remote Supervisor Adapter” on page 3.
To set the remote alert attempts on the ASM processor, log into the ASM processor. For more information, see “Logging into the ASM processor” on page 6.
2. In the navigation frame, select **Alerts** and scroll down to the Global Remote Alert Settings section.

Global Remote Alert Settings ⓘ

These settings apply to all remote alert recipients.

Remote alert retry limit: 5 times

Delay between retries: 0.5 minutes

Include event log with e-mail alerts

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 option to specify the number of additional times that the Remote Supervisor Adapter or ASM processor will attempt to send an alert to a recipient.

Delay between retries

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

3. Click **Save**.

Continue with the “Setting remote alerts” procedure.

Setting remote alerts

You can set remote alerts only when logged into the ASM processor. Complete the following steps to select the remote alerts to be sent:

1. Log into the Remote Supervisor Adapter. For more information, see “Logging into the Remote Supervisor Adapter” on page 3.
2. Log into the ASM processor. For more information, see “Logging into the ASM processor” on page 6.
3. In the navigation frame, select **Alerts** and scroll down to the Monitored Alerts section.
4. Select the events you want the ASM processor 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 6. 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 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 7. 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.

Note: Hard disk drive Predictive Failure Analysis[®] (PFA) alerts are not monitored.

Table 8. 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

5. Click **Save**.

Continue with "Setting local events" on page 37.

Setting local events

Complete the following steps to select the local events to which the ASM processor will respond:

1. Log into the Remote Supervisor Adapter. For more information, see “Logging into the Remote Supervisor Adapter” on page 3.
2. Log into the ASM processor. For more information, see “Logging into the ASM processor” on page 6.
3. In the navigation frame, click **Alerts** and scroll down to the Monitored Local Events section.
4. Select the events that you want to store in the event log. The ASM processor stores the notification only in the event log.

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 9. 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.

5. Click **Save**.

Configuring the serial ports

The ASM processor uses the two serial ports on the rear of your server. One of these serial ports can be shared with the server operating system while the other is dedicated to the ASM processor. The Remote Supervisor Adapter has a single serial port, dedicated to system management, which is always available for dial-in and dial-out alerting purposes. You will not be able to monitor it on the network operating system (NOS) or in any other applications.

Complete the following steps to configure your serial port. You can configure the serial ports on either the Remote Supervisor Adapter or the ASM processor, depending on

which device you are using. For more information on your serial port, see “Configuring PPP access over a serial port” on page 43. Configuring PPP access over a serial port only applies to the Remote Supervisor Adapter.

1. Log into the Remote Supervisor Adapter. For more information, see “Logging into the Remote Supervisor Adapter” on page 3.

To configure the serial ports on the ASM processor, log into the ASM processor. For more information, see “Logging into the ASM processor” on page 6.

2. In the navigation frame, click **Serial Port**. A window similar to the following opens:

The screenshot shows a configuration window titled "Serial Port" with two sections: "Serial Port 1" and "Serial Port 2". Each section contains the following settings:

- Baud rate: 57600 (dropdown menu)
- Parity: NONE (dropdown menu)
- Stop bits: 1 (dropdown menu)
- Dedicate to ASM
- [Advanced Modem Settings](#)

At the bottom right of the window is a "Save" button.

Note: Only Serial Port 1 appears on the Serial Port page when you are logged into the Remote Supervisor Adapter.

3. 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. 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. Check the **Dedicate to ASM** check box to reserve serial port 1 for the ASM processor. This option only appears when you are logged into the ASM processor. If shared with the operating system, the serial port serves the ASM processor only when 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 ASM processor take over the port from the NOS to dial-out and transmit an alert. The port then remains under ASM processor control until the server is restarted.

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 ?

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&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 10. 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.
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 ATS0=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 ATS0=0.

Table 10. Port 1 settings.

Field	What you type
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:

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

Configuring network interfaces

On the Network Interfaces page, 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 Remote Supervisor Adapter

You can configure an Ethernet connection to the Remote Supervisor Adapter when you are logged into the Remote Supervisor Adapter. Complete the following steps to configure your Ethernet setup:

1. Log into the Remote Supervisor Adapter. For more information, see “Logging into the Remote Supervisor Adapter” on page 3.
2. In the navigation frame, click **Network Interfaces**. A window similar to the following opens.

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

Ethernet ?

Interface

DHCP

Hostname

Static IP Configuration

IP address

Subnet mask

Gateway address

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

3. If you want to use an Ethernet connection, select **Enabled** in the Interface field. 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 Name field on the System page) do not automatically share the same name because the Name field is limited to 15 characters while the Hostname 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 24.

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 **Save**.
 10. Click **Advanced Ethernet Setup** if you need to set additional Ethernet settings.

Advanced Ethernet Setup

Data rate

Duplex

Maximum transmission unit bytes

Locally administered MAC address

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 Setup window.

Table 11. Advanced Ethernet setup.

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

Table 11. Advanced Ethernet setup.

Field	Function
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. Click **IP Configuration Assigned by the DNCP Server** to view the DHCP server-assigned settings.

A new page opens with a table that lists the host name, IP address, gateway IP address, subnet mask, domain name, DHCP server IP address, and up to three DNS server IP addresses.

IP Configuration Assigned by DHCP Server ?

Host name:
 IP address: 0.0.0.0
 Gateway address: 0.0.0.0
 Subnet mask: 0.0.0.0
 Domain name:

DNS Server IP Addresses

Primary: 0.0.0.0
 Secondary: 0.0.0.0
 Tertiary: 0.0.0.0

DHCP Server ?

IP address: 0.0.0.0

Cancel

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. You must be logged into the Remote Supervisor Adapter to configure PPP access over a serial port.

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. For more information, see “Logging into the Remote Supervisor Adapter” 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 the **Restart ASM** link to activate the changes.

Configuring network protocols

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

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

Configuring SNMP

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 *IBM Remote Supervisor Adapter Installation Guide*.

Complete the following steps to configure your SNMP:

1. Log into the Remote Supervisor Adapter. For more information, see “Logging into the Remote Supervisor Adapter” 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 24.
3. In the navigation frame, click **Network Protocols**. A window similar to the following opens:

Simple Network Management Protocol (SNMP)

SNMP agent: Disabled

SNMP traps: Disabled

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 24.
- 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.

5. 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 are incorrect, 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.

6. In the Community Name field, enter a name or authentication string that corresponds to the desired community.
7. In the corresponding Host Name or IP Address field, enter the host name or IP addresses of each community manager.
8. Click **Save**.
9. In the navigation frame, click the **Restart ASM** link to activate the changes.

Configuring DNS

Use this field 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 “Logging into the Remote Supervisor Adapter” on page 3.
2. In the navigation frame, click **Network Protocols** and scroll to the Domain Name System (DNS) section.

Domain Name System (DNS) ?

DNS

DNS server IP address 1

DNS server IP address 2

DNS server IP address 3

Host Table (IP Address to Host Name Mappings)

	IP Address	Host Name
1.	<input type="text" value="0.0.0.0"/>	<input type="text"/>
2.	<input type="text" value="0.0.0.0"/>	<input type="text"/>
3.	<input type="text" value="0.0.0.0"/>	<input type="text"/>
4.	<input type="text" value="0.0.0.0"/>	<input type="text"/>

3. 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.
4. Enter the IP address of up to three DNS servers in the DNS server IP address fields.
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.
5. 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.
6. 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.
7. Click **Save**.
8. 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. For more information, see “Logging into the Remote Supervisor Adapter” on page 3.
2. In the navigation frame, click **Network Protocols** and scroll down to the Simple Mail Transfer Protocol (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.

Using the configuration file

When logged into the Remote Supervisor Adapter, select **Configuration File** in the navigation bar to:

- Backup ASM configuration
- Restore ASM configuration

The screenshot shows a web interface with two main sections. The top section is titled "Backup ASM Configuration" and contains a help icon, a paragraph of instructions, a blue link "view the current configuration summary", and a "Backup" button. The bottom section is titled "Restore ASM Configuration" and contains a help icon, a paragraph of instructions, a text input field labeled "Select configuration file to restore", a "Browse..." button, and "Restore" and "Modify and Restore" buttons.

Backing up your current Remote Supervisor Adapter configuration

You can download a copy of your current Remote Supervisor Adapter 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. For more information, see "Logging into the Remote Supervisor Adapter" 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

Use this section to restore a saved configuration from a file. You can restore the saved configuration in full, or you can modify key fields in the saved configuration before restoring them to your ASM configuration. Modifying the configuration before restoring it is helpful when setting up multiple ASM processors with similar configurations. This enables you to quickly specify parameters that require unique values such as names and IP addresses without having to re-enter common, shared information.

Complete the following steps to restore your current configuration:

1. Log into the Remote Supervisor Adapter. For more information, see “Logging into the Remote Supervisor Adapter” 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 ASM defaults

The **Restore Defaults** link enables you to restore the default configuration of the Remote Supervisor Adapter or the ASM processor, depending on which one you have accessed. You can perform this function only if you have read/write access.

Attention: When you click **Restore Defaults**, all configuration settings will be lost.

In the navigation frame, click **Restore Defaults** to restore the default settings of the Remote Supervisor Adapter or the ASM processor, depending on which one you have accessed. If you logged into the Remote Supervisor Adapter, you will lose your TCP/IP connection and must reconfigure the network interface to restore connectivity.

Restarting ASM

The **Restart ASM** link enables you to restart the Remote Supervisor Adapter or the ASM processor, depending on which you have accessed. You can perform this function only if you have read/write access. Any TCP/IP, modem, or interconnect connections are temporarily dropped. You must login again to use the ASM Web interface.

Logging off

The **Log Off** or **Log off Remote ASM** link enables you to log off the Remote Supervisor Adapter or the ASM processor, depending on which one you have accessed.

1. Click **Log Off** in the navigation frame.

Note: If you are logged into the ASM processor, click **Log off Remote ASM** in the navigation frame. You return to the Remote Supervisor Adapter.

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 remains 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.

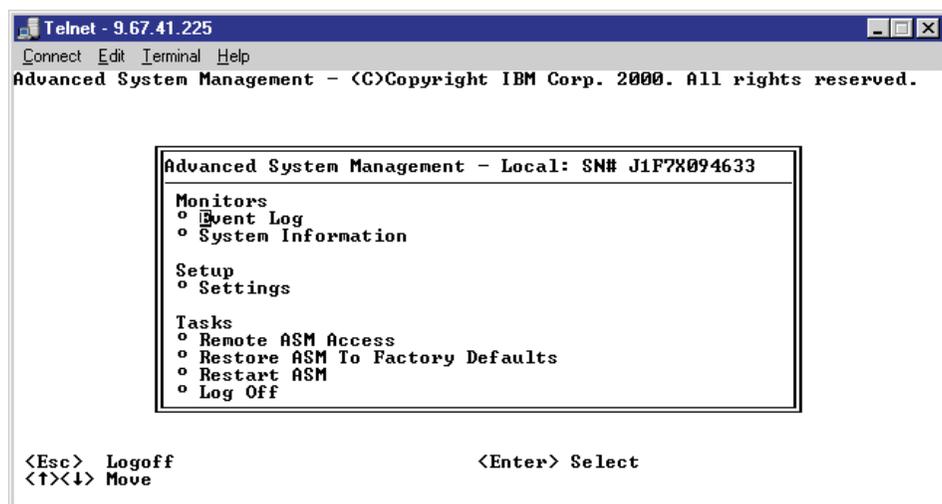
Note: F1 through F4 are the only function keys that are supported in the text-based interface.

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 53.
4. Type a username 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.



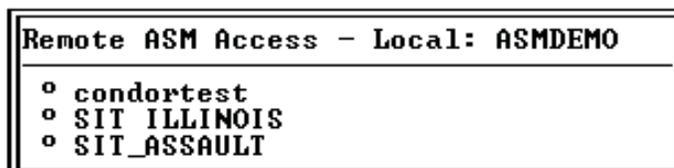
Note: Press the Up Arrow and Down Arrow keys to navigate this screen. Press Esc to exit to the Advanced System Management window; if you press Esc at the Advanced System Management window, you log off from your session. Press F3 to exit the window you are viewing.

Accessing remote adapters through an ASM interconnect network

You can connect to remote systems through the ASM interconnect network on the Remote ASM Access window.

Complete the following steps to access remote Remote Supervisor Adapters:

1. 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.



2. Select a processor or adapter. The Remote ASM Login window opens.
3. Enter your username 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.
4. 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.

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 12. COM properties.

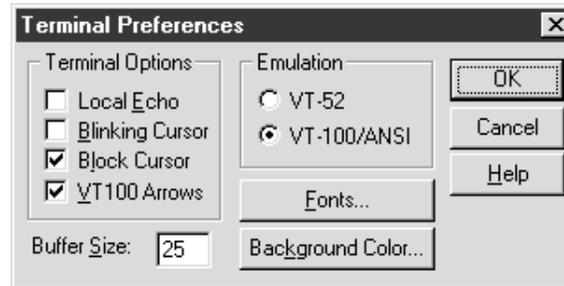
Field	Entry
Bits per second	57600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

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.

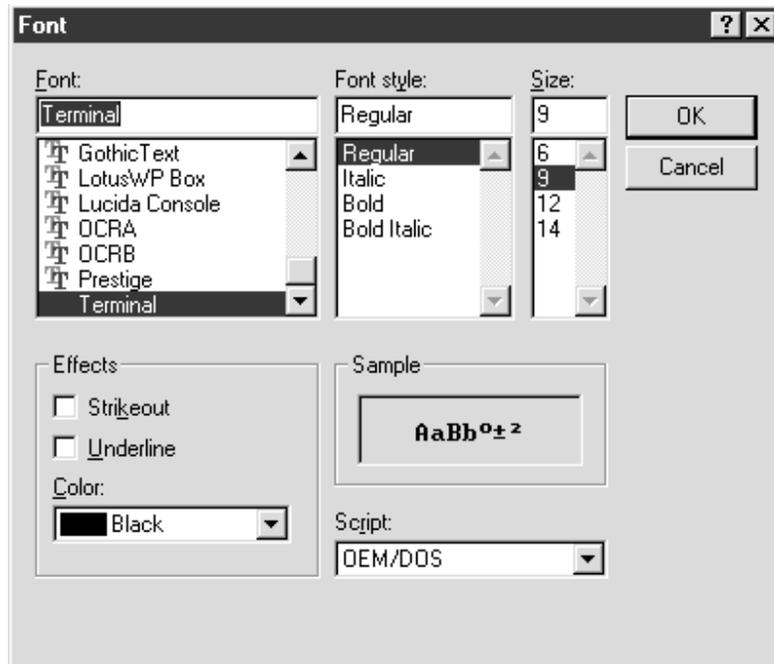
Configuring terminal settings

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 or ASM processor 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. The monitoring features available to you depend on whether you are logged into the Remote Supervisor Adapter or the ASM processor.

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 and Alert Profiles window, you can:

- Set login profiles to control access
- 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 event log attachments when alerts are generated

From the Serial Port windows, you can:

- Configure the serial port
- Configure advanced modem settings

From the Network Interfaces/Protocols window, you can:

- Set up an Ethernet connection
- Set up a PPP over serial port connection
- Configure SNMP setup
- Configure DNS setup
- Configure SMTP setup

From the ASM Processor Clock window, you can set the ASM date and time.

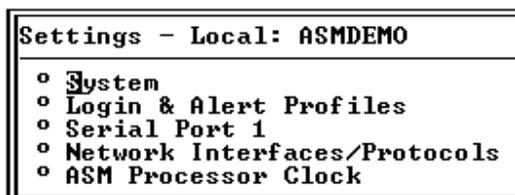
Setting system information

You can set the system name and ID number.

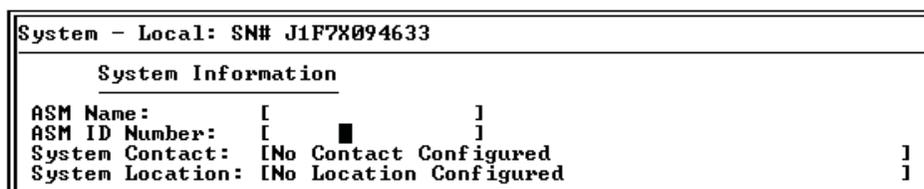
Setting Remote Supervisor Adapter system information

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 51.
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 the Remote Supervisor Adapter” on page 75.
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 Remote Supervisor Adapter system information

Complete the following steps to set your ASM processor system information:

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 51.
2. Log into the ASM processor. For more information, see “Accessing remote adapters through an ASM interconnect network” on page 52.
3. 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
```

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

```
System - Remote: RGR316224026
├─ System Information
├─ ASM Name: [RGR316224026 ]
├─ Server Timeouts
├─ POST Watchdog (mins): <Disabled>
├─ Loader Watchdog (mins): <Disabled>
├─ O/S Watchdog (mins): <Disabled>
└─ Power Off Delay (mins): <1.0>
```

5. 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 the Remote Supervisor Adapter” on page 75.

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 51.
2. Log into the ASM processor. For more information, see “Accessing remote adapters through an ASM interconnect network” on page 52.
3. In the Advanced System Management window, select **System Settings**.
4. In the System Settings window, select **System**. A window similar to the following opens:

```
System - Remote: RGR316224026
-----
System Information
ASM Name: [RGR316224026 ]
Server Timeouts
POST Watchdog (mins): <Disabled>
Loader Watchdog (mins): <Disabled>
O/S Watchdog (mins): <Disabled>
Power Off Delay (mins): <1.0>
```

5. In the System window, use the Down Arrow key to move to the Server Timeouts section. You can set the Remote Supervisor Adapter to 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
6. Enable the server timeouts that correspond to the events you want the Remote Supervisor Adapter to respond to.

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 on only 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 O/S watchdog feature requires that the ASM processor 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 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 both the IBM Director with UM Server Extensions agent code and the ASM processor device driver 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 ASM processor, see the *UM Server Extensions User's Guide*.

Creating login profiles

The Login Profiles table enables you to view a summary list of all login profiles. Use the options in the Login ID column to configure individual login profiles. You can define up to twelve unique profiles. Each login profile in the Login ID column is labeled with the configured login ID for that particular profile. If you have not configured a profile, the name of the login profile by default will be ~ not used ~.

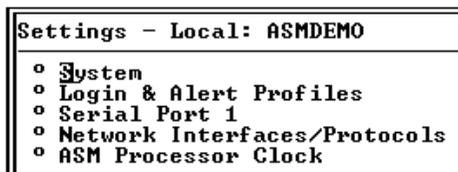
To work with a login profile, click the profile to open a profile setup details page.

Note: By default, the ASM subsystem comes configured with one login profile that enables remote access using a login 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 ASM subsystem.

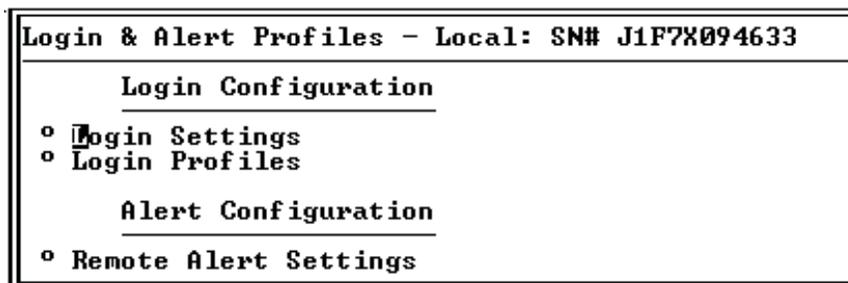
Creating a login profile on the Remote Supervisor Adapter

Complete the following steps to configure a login profile:

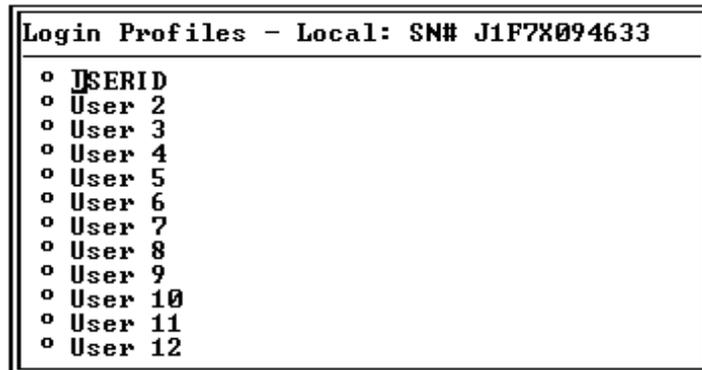
1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 51.
2. In the Advanced System Management window, select **Settings**. The Settings window opens:



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

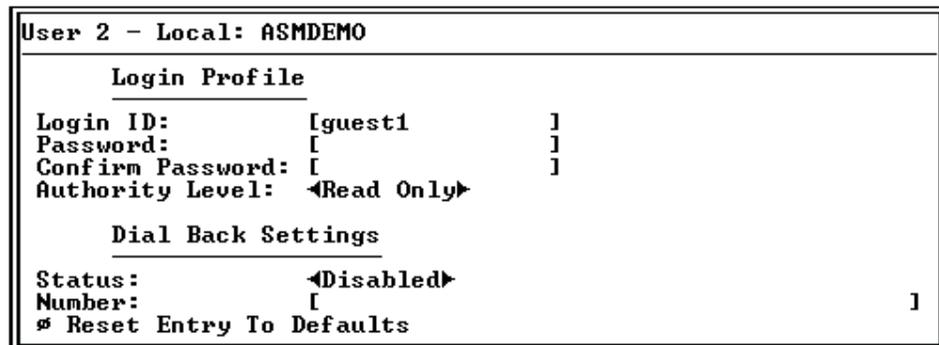


- In the Login and Alert Profiles section, select **Login Profiles**.



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:



- 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.

- 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.

- 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.

9. 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 11 on page 64.

Note: If this menu is enabled, you must enter a phone number in the Number field of this profile.

10. In the Number field, type the phone number for the Remote Supervisor Adapter to use when dialing back.

This phone number is dialed when the user successfully logs into the Remote Supervisor Adapter.

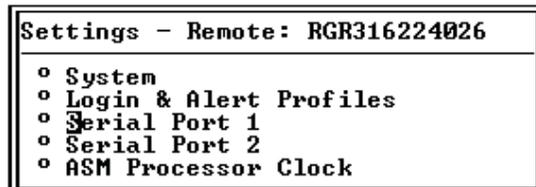
Note: By default, the ASM subsystem comes configured with one login profile that enables remote access using a login ID of USERID and a password of PASSWORD (the 0 is a zero). To avoid a potential security exposure, change this default login profile during the initial setup of the Remote Supervisor Adapter.

11. 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.

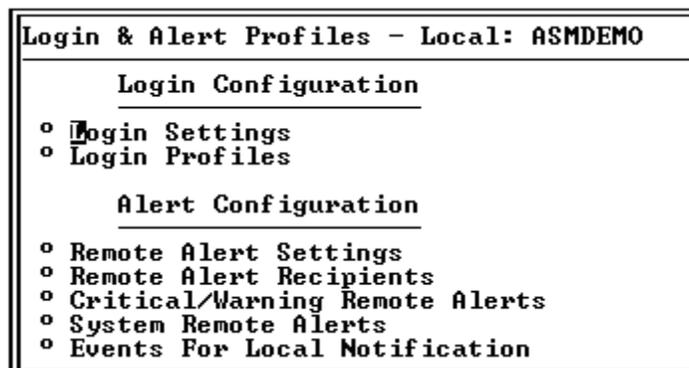
Creating a login profile on the ASM processor

Complete the following steps to configure a login profile:

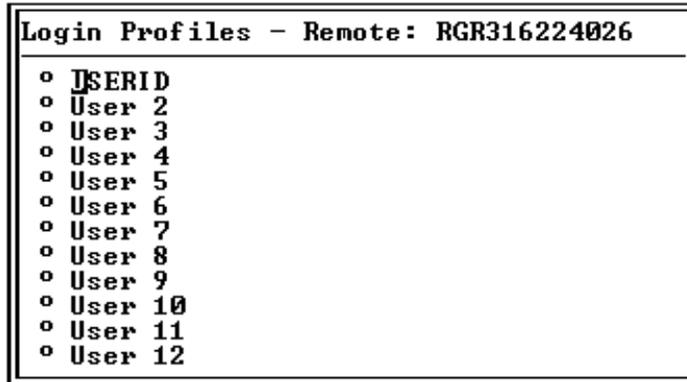
1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 51.
2. Log into the ASM processor. For more information, see “Accessing remote adapters through an ASM interconnect network” on page 52.
3. In the Advanced System Management window, select **Settings**. The Settings window opens:



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

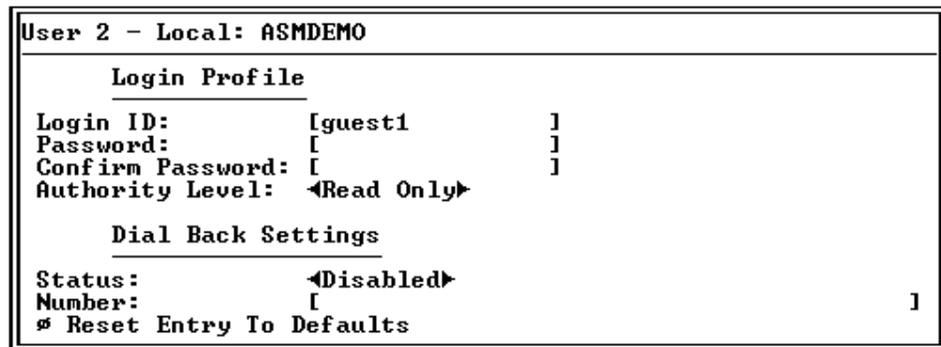


- In the Login and Alert Profiles section, select **Login Profiles**.



Use the Login Profiles window to view, configure, or change individual login profiles. You can define up to 12 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:



- 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.

- 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 nonalphanumeric 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.

- 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.

10. 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 12.

Note: If this menu is enabled, you must enter a phone number in the Number field of this profile.

11. In the Number field, type the phone number for the Remote Supervisor Adapter to use when dialing back.

This phone number is dialed when the user successfully logs into the Remote Supervisor Adapter.

Note: By default, the ASM subsystem comes configured with one login profile that enables remote access using a login 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 the initial setup of the Remote Supervisor Adapter.

12. 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 51.

To set modem and dial-in settings on the ASM processor, log into the ASM processor. For more information, see “Accessing remote adapters through an ASM interconnect network” on page 52.

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

Login Settings - Local: ASMDEMO	
Dial-in Support Status:	◀Disabled▶
Delay before next Login after Failed Attempt <mins>:	◀2.0▶

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 names to view, configure, or change individual alert recipients. You can define up to twelve unique recipients. Each alert recipient is labeled with the recipient name.

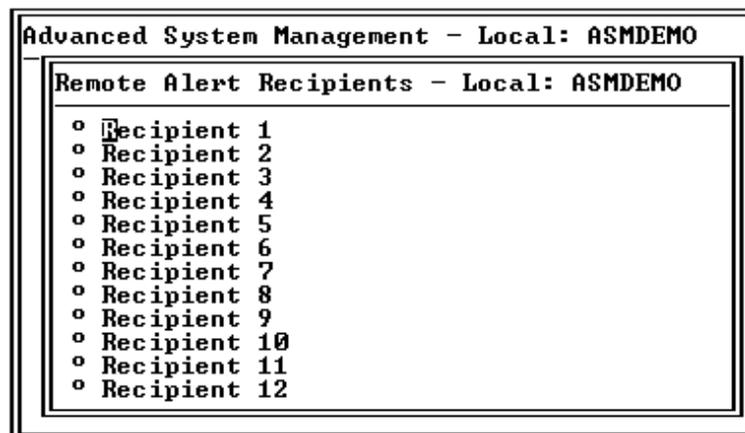
When you configure a remote alert entry, the Remote Supervisor Adapter, ASM processor, or ASM PCI adapter sends an alert to a remote system (through a serial connection or a network connection), a numeric pager, or an alphanumeric pager when an event selected from the Enabled Alerts group occurs. This 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 80.

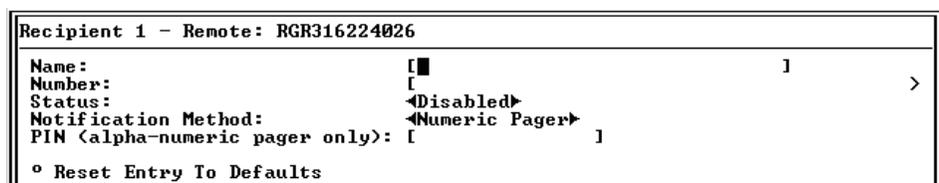
Note: You cannot distinguish between what alerts will be sent to which remote alert recipient. All configured recipients receive each alert you select.

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 51.
2. Log into the ASM processor. For more information, see “Accessing remote adapters through an ASM interconnect network” on page 52.
3. Select **Settings**.
4. Select **Login & Alert Profiles**.
5. In the Login and Alert Profiles window, select **Remote Alert Recipients**.



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



7. 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.
8. 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.

9. In the Status field, select **Enabled**. This field enables you to activate or deactivate remote alert recipients.
10. Select **Enabled** in the Receive critical alerts only field if you want the recipient to receive only critical alerts.
11. 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. For more information on installing UM Server Extensions code for the ASM processor, see the *UM Server Extensions User's Guide*.

12. If you chose alphanumeric pager as the notification method, enter the PIN in the PIN (alpha-numeric pager only) field.
13. If you select the E-mail over PPP or SNMP over PPP notification methods, type the login ID needed to log into the dial-up service account of the recipient 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 onto the IBM Global Network IP Remote Access Service Provider, the PPP login ID should contain information in the following format: Secureip.X.Y, where 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 47.

14. 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 log into the dial-up service account. You must fill in this field for the E-mail over PPP and SNMP over PPP notification methods.

15. 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.

16. 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 51.

To set remote alert attempts on the ASM processor, log into the ASM processor. For more information, see “Accessing remote adapters through an ASM interconnect network” on page 52.

2. Select **Settings**.
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 or ASM processor will attempt to forward an alert to a recipient. 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 or ASM processor will wait between retries to send an alert to a recipient.
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 68 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 51.
2. Log into the ASM processor. For more information, see “Accessing remote adapters through an ASM interconnect network” on page 52.
3. Select **Settings**.
4. Select **Login & Alert Profiles**.
5. In the Login and Alert Profiles window, select Critical/Warning Remote Alerts.

Critical/Warning Remote Alerts - Local: ASMDEMO	
<u>Critical Alerts</u>	
Hard Disk Drive:	◀Disabled▶
Multiple Fan Failure:	◀Disabled▶
Power Failure:	◀Disabled▶
Tamper:	◀Disabled▶
Temperature:	◀Disabled▶
Voltage:	◀Disabled▶
URM Failure:	◀Disabled▶
<u>Warning Alerts</u>	
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 13. 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

Table 13. Critical remote alerts.

Event	Action	Numeric code
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 14. 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[®] (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 15. 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

Table 15. System remote alerts.

Event	Action	Numeric code
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

7. Press F3 and select **Events For Local Notification**.
8. Select the events that you want to store in the event log. The ASM processor stores the notification only in the event log.

Local events

Eventually, local events will be sent to the server where the ASM processor resides. These events will not be sent to remote alert recipients.

Table 16. 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.
PFA	Generates a local notification if any of the hardware in the system generates a PFA.

Configuring the serial port

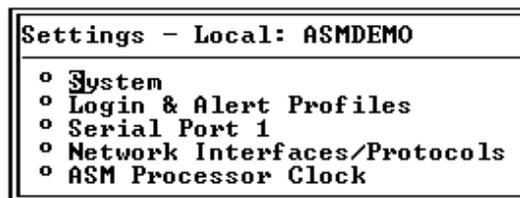
The ASM processor uses the two serial ports on the rear of your server. One of these serial ports can be shared with the server operating system while the other is dedicated to the ASM processor. The Remote Supervisor Adapter has a single serial port, dedicated to system management, which is always available for dial-in and dial-out alerting purposes. You will not be able to view it 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.

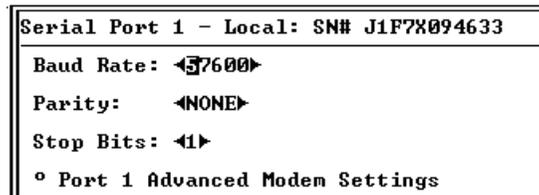
Configuring the serial port in the Remote Supervisor Adapter

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 78.

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 51.
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 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.

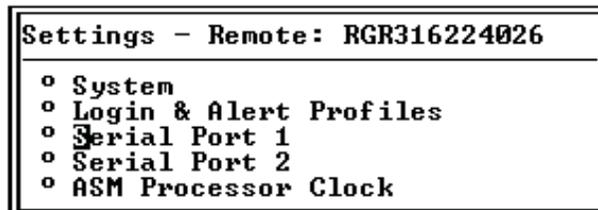
Table 17. Port 1 settings.

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 one ring 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.
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.

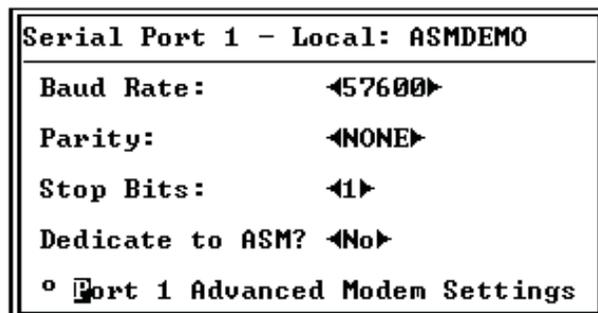
Configuring the serial ports in the ASM processor

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 78.

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 51.
2. Log into the ASM processor. For more information, see “Accessing remote adapters through an ASM interconnect network” on page 52.
3. In the Advanced System Management window, select **Settings**. The Settings window opens:



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



5. 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.

6. 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.

7. 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).

8. 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 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.

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

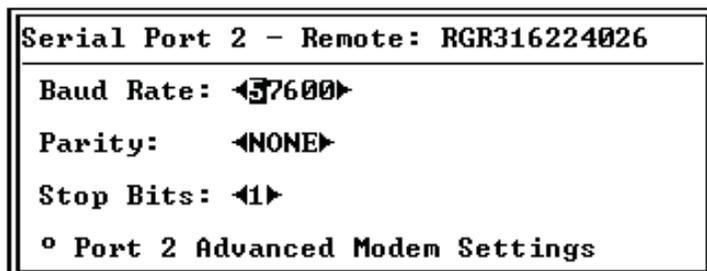
Set these values only if the alert forwarding functions are not working properly. The strings marked with an asterisk (*) require a carriage return (^M) to be manually entered at the end of the field value.

The following table describes the initialization strings for this modem.

Table 18. 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.
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.

10. Press F3 and then select Serial Port 2 to configure the second serial port.



The same fields appear in the Serial Port 2 window, but you cannot dedicate serial port 2 to the ASM processor. Repeat steps 6 through 9 to configure serial port 2.

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:

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

Configuring network interfaces

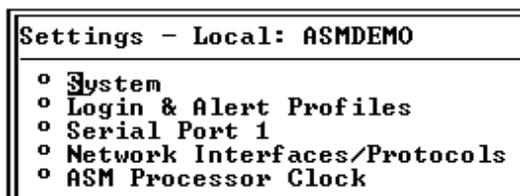
With the network interface options, you can set access to the Remote Supervisor Adapter by:

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

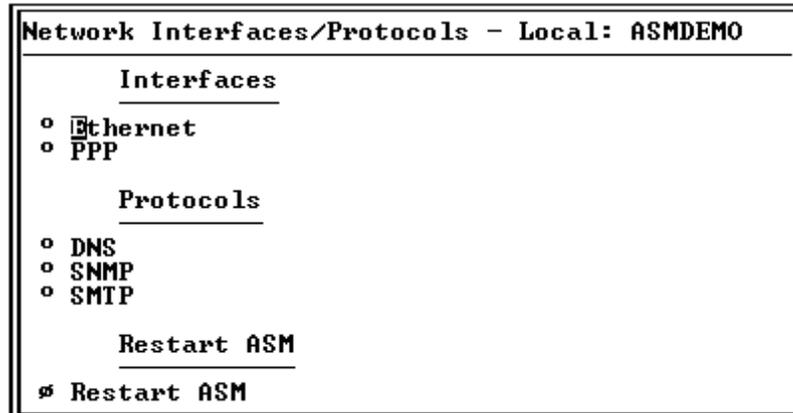
Configuring an Ethernet connection to the Remote Supervisor Adapter

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 51.
2. In the Advanced System Management window, select **Settings**. The Settings window opens:

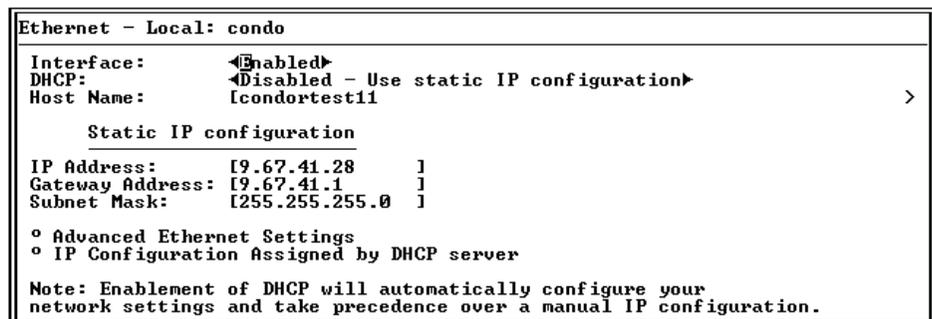


- In the Settings window, select **Network Interfaces/Protocols**. The following window opens:



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

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



- In the Interface field, select **Enabled**. It is enabled by default.
 - 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.
- 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:

- 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 56.

- 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 the DHCP server to allow the use of this hostname.
 - If the **Hostname** field is not set, then the Remote Supervisor Adapter DHCP support will request the DHCP server to 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 19. 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>Full Enables data to be carried in both directions at once.</p> <p>Half 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 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.

1. Log into the Remote Supervisor Adapter. For more information, see "Accessing a text-based interface via a TELNET connection" on page 51.
2. 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.

```

PPP - Local: ASMDEMO
-----
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, 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
5. 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
6. 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
7. In the Authentication field, specify the type of authentication protocol that will be negotiated when a PPP connection is attempted.
 - The **PAP Only** setting uses a two-way handshake procedure to validate the identity of the originator of 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 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. 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.

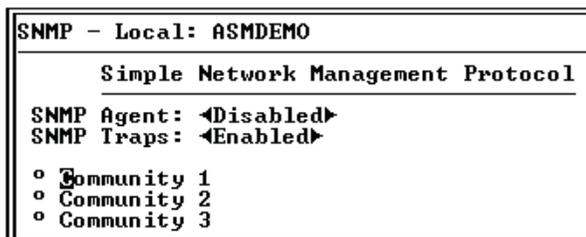
Note: If you are planning to configure SNMP trap alerts on the Remote Supervisor Adapter, you must install and compile the supplied management information base (MIB) on your SNMP manager. For more information on the MIB file, see your Remote Supervisor Adapter Installation Guide.

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 51.
2. 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 56.

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

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



5. 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.

6. 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.

7. In the Name field, enter the name or authentication string that corresponds to the desired community.
8. In the corresponding Host Name1 or IP Address1 field for this community, type the host name or IP addresses of this community.
9. 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 51.
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 host-names.

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 51.
2. In the Network Interfaces/Protocols window, select **SMTP**. The SMTP window opens:

SMTP - Local: ASMDemo	
<u>Simple Mail Transfer Protocol</u>	
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 date and time

The Remote Supervisor Adapter and the ASM processor contain internal clocks. Setting one does not affect the settings on the other, and each serve separate purposes.

Setting the date and time on the Remote Supervisor Adapter

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

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 51.
2. In the Advanced System Management window, select **Settings**.
3. In the Settings window, select **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.

```

ASM Processor Clock - Local: SN# J1F7X094633

Clock Settings
Time <hh:mm:ss> : [03]:[29]:[45]
Date <mm/dd/yyyy>: [01]/[08]/[2000]

Time Zone Settings
Offset from GMT : <0:00>
Observe daylight saving time? <No>

```

The Remote Supervisor Adapter has a 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 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.

4. 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.
5. Set the time zone settings, depending on your location.

GMT offset

Use the Offset from GMT field to specify the 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 automatically adjust when DST changes.

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

Setting the date and time on the ASM processor

Complete the following steps to set the ASM processor clock:

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 51.
2. Log into the ASM processor. For more information, see “Accessing remote adapters through an ASM interconnect network” on page 52.
3. In the Advanced System Management window, select **Settings**.
4. In the Settings window, select **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 for the ASM processor, which is independent of the date and time settings of the clock on the server system board.

```

ASM Processor Clock - Remote: RGR316224026

Clock Settings
Time <hh:mm:ss> : [17]:[33]:[10]
Date <mm/dd/yyyy>: [08]/[06]/[2001]

```

The ASM processor 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. You can

remotely access the battery-backed event log even if the system is turned off or otherwise disabled. This facilitates immediate problem determination and resolution.

5. 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.
6. 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 automatically adjust when DST changes.

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

Chapter 8. Text-based interface 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 51.
2. Log into the ASM processor. For more information, see “Accessing remote adapters through an ASM interconnect network” on page 52.
3. 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
```

4. 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 53.

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.

5. 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 65.

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.

6. 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 Remote Supervisor 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.

Viewing the Remote Supervisor Adapter event log

The Remote Supervisor Adapter event log displays Remote Supervisor Adapter-specific data, such as:

- Resets and bootups
- Interconnect connections
- Firmware updates

Complete the following steps to access and view the Remote Supervisor Adapter event log:

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 51.
2. In the Advanced System Management window, select **Event Log**.

```

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.

```

3. Select **View Event Log** to view the history of Remote Supervisor Adapter and ASM processor logins.

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 the ASM processor event log

Complete the following steps to access and view the ASM processor event log.

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 51.
2. Log into the ASM processor. For more information, see “Accessing remote adapters through an ASM interconnect network” on page 52.
3. In the Advanced System Management window, select **Event Log**.
4. Select **View Event Log** to view the two most recent events on your server.

```

View Event Log - Remote: RGR316224026
Date:08-06-01 Time:17:33:01 Severity:I Source:SERUPROC
Remote Login Successful User ID = USERID
Date:08-06-01 Time:17:33:01 Severity:I Source:SERUPROC
System SN# J1F7X094633 started a RS485 connection with us
o View next log entries.

```

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.

5. Select **View next log entry** to view the next two entries or press F3 to return to the Event Log window.
6. To clear the event log of all current entries, select **Clear event log**.

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.

Viewing VPD for the Remote Supervisor Adapter

Complete the following steps to view the firmware VPD for 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 51.
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)**.
4. Select **ASM VPD** in the VPD window. The ASM VPD windows opens:

ASM VPD - Local: SN# J1F7X094633			
	Application Firmware	Boot ROM Firmware	Remote Control Firmware
Build ID	FBET05-	FBBR05-	FBRG05-
Revision	16	16	16
File Name	CNETMNUS.PKT	CNETBRUS.PKT	CNETRGUS.PKT
Release Date	07-26-01	07-26-01	07-26-01

5. Press F3 to return to the System Information window.

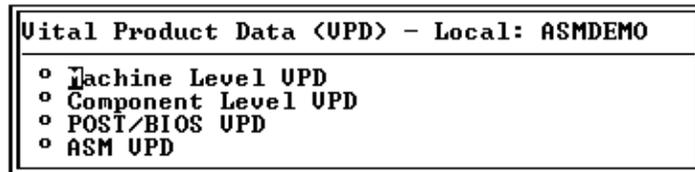
Viewing VPD for the ASM processor

Complete the following steps to view the ASM processor VPD.

1. Log into the Remote Supervisor Adapter. For more information, see “Accessing a text-based interface via a TELNET connection” on page 51.
2. Log into the ASM processor. For more information, see “Accessing remote adapters through an ASM interconnect network” on page 52.
3. In the Advanced System Management window, select **System Information** to view the status of the hardware and software components on the server.

System Information - Remote: RGR316224026	
o	Vital Product Data (VPD)
o	Component Activity Log

4. Select **Vital Product Data (VPD)**. The Vital Product Data (VPD) window opens:



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

Machine level VPD

The VPD for the system is displayed in this window.

Table 20. 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.

Component level VPD

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

Table 21. 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 22. 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.

Remote Supervisor Adapter system data

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

Table 23. Remote Supervisor Adapter vital product data.

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

6. Press F3 to return to the System Information window.
7. Select **Component Activity Log**. You can find a record of component activity.

Table 24. 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.

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.

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. For more information on accessing a remote adapter, see “Accessing remote adapters through an ASM interconnect network” on page 52.

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 server text console

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 a 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.

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 **Restart ASM** link enables you to restart the Remote Supervisor Adapter or the ASM processor, depending on which you have accessed. You can perform this function only if you have read/write access. Any TCP/IP, modem, or interconnect connections are temporarily dropped. You must 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**.

If you are logged into the ASM Processor, you must first select **Log Off Remote ASM**.

2. Click **Yes**.

Appendix A. Getting help, information 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/cgi-bin/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 Help-Center[®]. 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 time will vary depending on the number and complexity of incoming calls.

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	02-482 9202
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.

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.

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 in the United States, other countries, or both.

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

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

Important notes

Processor speeds indicate the internal clock speed of the microprocessor; other factors also affect application performance.

CD-ROM drive speeds list the variable read rate. Actual speeds vary and are often less than the maximum possible.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for approximately 1000 bytes, MB stands for approximately 1000000 bytes, and GB stands for approximately 1000000000 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity may vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard disk drive bays with the largest currently supported drives available from IBM.

Maximum memory may require replacement of the standard memory with an optional memory module.

IBM makes no representation or warranties regarding non-IBM products and services that are ServerProven, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. These products are offered and warranted solely by third parties.

Unless otherwise stated, IBM makes no representations or warranties with respect to non-IBM products. Support (if any) for the non-IBM products is provided by the third party, not IBM.

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

Index

A

- alerts 8
- ASM
 - time setting 27, 28
- ASM configuration, restoring 49
- ASM defaults, restoring 49
- ASM interconnect network
 - accessing remote adapters 18
- ASM interconnect network, accessing remote adapters 52, 90
- ASM processor
 - clock setting 83
 - date setting 27
 - login profiles
 - creating 30
- ASM processor event log 14
- ASM processor event log, viewing 87
- ASM processor firmware 18
- ASM processor login profiles
 - creating 62
- ASM processor serial ports, configuring 73
- ASM processor system information, setting 57
- ASM processor VPD, viewing 88
- ASM, restarting 49

C

- configuration
 - backups 48
- configuring SNMP 45
- critical events 10

D

- delay between retries, setting 34
- Domain Name System (DNS), configuring 46, 81

E

- emote alert attempts 34
- Ethernet connection, configuring 75
- event log
 - viewing 13, 86
 - error 14
 - informational 13
 - machine level VPD 15
 - POST/BIOS data 15
 - system data 16
 - warning 13

F

- factory defaults, restoring 91
- Fan Speeds section 13
- firmware update 17

I

- initialization-string guidelines 40, 75

L

- local events
 - setting 37
- Logging into the ASM processor 6
- Logging into the Remote Supervisor Adapter 3
- logging off 5, 8, 50, 91
- login profile
 - read-only 29, 31
 - read/write 29, 31
- login profiles 7

N

- notes, important 98
- notices and statements 2

P

- power 10
- power-off delay 59
- PPP access
 - serial port, configuration 43

R

- remote alert
 - settings, warning alerts 36
- remote alert attempts
 - setting 67
- remote alert recipients
 - configuring 65
- remote alert retry limit, setting 34
- remote alert settings 32
- remote alerts
 - setting, critical alerts 35
- remote alerts, setting 35, 68
- remote control server power
 - O/S shutdown 21
 - power off server immediately 21
 - power on server immediately 21
 - restart server immediately 21

- Remote server system health 9
- remote servers
 - monitoring 10
 - temperature 10
 - thresholds 12
 - voltage 12
- Remote Supervisor Adapter
 - clock setting 82
 - date setting 27
 - Ethernet connection, configuration 40
 - login profiles
 - creating 28
 - server timeouts, setting 25
 - system information, setting 24
 - tasks 17
- Remote Supervisor Adapter event log 13
- Remote Supervisor Adapter event log, viewing 86
- Remote Supervisor Adapter features 1
- Remote Supervisor Adapter firmware 17
- Remote Supervisor Adapter login profiles
 - creating 60
- Remote Supervisor Adapter serial port, configuring 71
- Remote Supervisor Adapter system information, setting 56
- Remote Supervisor Adapter VPD, viewing 88

S

- serial port access, configuring 78
- serial ports, configuring 37
- Server Power and Restart Activity section 20
- Server Power/Restart Activity section 10
- server timeouts
 - setting 58
- service summary 93
- settings
 - dial-in 31, 64
 - modem 31, 64
- Simple Mail Transfer Protocol (SMTP) configuration 82
- Simple Mail Transfer Protocol (SMTP), configuring 47
- simple network management protocol (SNMP), configuring 80
- SNMP, configuring 45
- state 10
- system alerts 36

T

- Temperature Thresholds window 11
- terminal settings 53
- text-based interface
 - accessing using TELNET 51
 - accessing via a direct serial connection 52
 - configuring for Remote Supervisor Adapter 55
 - monitoring
 - fans 85
 - voltage 85

- trademarks 98
- transfer files 8

V

- vital product data 7
 - viewing 14
- Voltage Thresholds window 12
- VPD, ASM processor and remote managed server 15
- VPD, Remote Supervisor Adapter 14

W

- watchdog
 - loader 59
 - o/s 59
 - post 58
- Web browser requirements 2



Part Number: 33P2529



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

33P2529

