Avaya Remote Supervisor Adapter

User Guide

(for use with Avaya S8500 Media Server)

555-245-702
Issue 1
November 2003

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support.

Preventing Toll Fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there may be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

How to Get Help

For additional support telephone numbers, go to the Avaya support Web site: http://www.avaya.com/support. If you are:

- Within the United States, click the *Escalation Management* link. Then click the appropriate link for the type of support you need.
- Outside the United States, click the *Escalation Management* link. Then click the *International Services* link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Standards Compliance

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment.

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

Safety of Information Technology Equipment, IEC 60950, 3rd Edition including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.

Safety of Information Technology Equipment, CAN/CSA-C22.2 No. 60950-00 / UL 60950, 3rd Edition

Safety Requirements for Customer Equipment, ACA Technical Standard (TS) 001 - 1997

One or more of the following Mexican national standards, as applicable: NOM 001 SCFI 1993, NOM SCFI 016 1993, NOM 019 SCFI 1998

The equipment described in this document may contain Class 1 LASER Device(s). These devices comply with the following standards:

- EN 60825-1, Edition 1.1, 1998-01
- 21 CFR 1040.10 and CFR 1040.11.

The LASER devices operate within the following parameters:

- Maximum power output: -5 dBm to -8 dBm
- Center Wavelength: 1310 nm to 1360 nm

Luokan 1 Laserlaite

Klass 1 Laser Apparat

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposures. Contact your Avaya representative for more laser product information.

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards and all relevant national deviations:

Limits and Methods of Measurement of Radio Interference of Information Technology Equipment, CISPR 22:1997 and EN55022:1998.

Information Technology Equipment – Immunity Characteristics – Limits and Methods of Measurement, CISPR 24:1997 and EN55024:1998, including:

- Electrostatic Discharge (ESD) IEC 61000-4-2
- Radiated Immunity IEC 61000-4-3
- Electrical Fast Transient IEC 61000-4-4
- Lightning Effects IEC 61000-4-5
- Conducted Immunity IEC 61000-4-6
- Mains Frequency Magnetic Field IEC 61000-4-8
- Voltage Dips and Variations IEC 61000-4-11
- Powerline Harmonics IEC 61000-3-2
- Voltage Fluctuations and Flicker IEC 61000-3-3

Federal Communications Commission Statement

Part 15:

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Part 68: Answer-Supervision Signaling

Allowing this equipment to be operated in a manner that does not provide proper answer-supervision signaling is in violation of Part 68 rules. This equipment returns answer-supervision signals to the public switched network when:

- answered by the called station,
- answered by the attendant, or
- routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user.

This equipment returns answer-supervision signals on all direct inward dialed (DID) calls forwarded back to the public switched telephone network. Permissible exceptions are:

- A call is unanswered.
- A busy tone is received.
- A reorder tone is received.

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

REN Number

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover of this equipment is a label that contains, among other information, the FCC registration number, and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

For G350 and G700 Media Gateways:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. The digits represented by ## are the ringer equivalence number (REN) without a decimal point (for example, 03 is a REN of 0.3). If requested, this number must be provided to the telephone company.

For all media gateways:

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0. To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company.

REN is not required for some types of analog or digital facilities.

Means of Connection

Connection of this equipment to the telephone network is shown in the following tables.

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/REN/ A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2-T	0.0B	RJ2GX, RJ21X
CO trunk	02GS2	0.3A	RJ21X
	02LS2	0.3A	RJ21X
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9-BN	6.0F	RJ48C, RJ48M
	04DU9-IKN	6.0F	RJ48C, RJ48M
	04DU9-ISN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9-DN	6.0Y	RJ48C

For G350 and G700 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/REN/ A.S. Code	Network Jacks
Ground Start CO trunk	02GS2	1.0A	RJ11C
DID trunk	02RV2-T	AS.0	RJ11C
Loop Start CO trunk	02LS2	0.5A	RJ11C
1.544 digital interface	04DU9-BN	6.0Y	RJ48C
	04DU9-DN	6.0Y	RJ48C
	04DU9-IKN	6.0Y	RJ48C
	04DU9-ISN	6.0Y	RJ48C
Basic Rate Interface	02IS5	6.0F	RJ49C

For all media gateways:

If the terminal equipment (for example, the media server or media gateway) causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242- 2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. It is recommended that repairs be performed by Avaya certified technicians.

The equipment cannot be used on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

This equipment, if it uses a telephone receiver, is hearing aid compatible.

Canadian Department of Communications (DOC) Interference Information

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

Declarations of Conformity

United States FCC Part 68 Supplier's Declaration of Conformity (SDoC)

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site: http://www.avaya.com/support.

All Avaya media servers and media gateways are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at: http://www.part68.org by conducting a search using "Avaya" as manufacturer.

European Union Declarations of Conformity

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (*Conformité Europeénne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC). This equipment has been certified to meet CTR3 Basic Rate Interface (BRI) and CTR4 Primary Rate Interface (PRI) and subsets thereof in CTR12 and CTR13, as applicable.

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site: http://www.avaya.com/support.

Japan

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

To order copies of this and other documents:

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.207.866.6701
FAX 1.800.457.1764 or 1.207.626.7269

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management

E-mail: totalware@gwsmail.com

For the most current versions of documentation, go to the Avaya support Web site: http://www.avaya.com/support.

Contents

About this book

Overview

This book, *Avaya Remote Supervisor Adapter User Guide*, 555-245-702, provides procedures to administer your Remote Supervisor Adapter (RSA) on the Avaya S8500 Media Server.

Audience

This book is for the customer administrator or other personnel who are responsible for configuration of the RSA.

Downloading this book and updates from the Web

You can download the latest version of this book from the Avaya Web site. You must have access to the Internet, and a copy of Acrobat Reader must be installed on your personal computer.

Avaya makes every effort to ensure that the information in this book is complete and accurate. However, information can change after we publish this book. Therefore, the Avaya Web site might also contain new product information and updates to the information in this book. You also can download these updates from the Avaya Web sit.

Downloading this book

To download the latest version of this book:

1. Access the Avaya Web site at http://support.avaya.com.
2. At the top center of the page, click **Product Documentation**.

   The system displays the Welcome to Production Documentation page.
3. In the upper-left corner, type the 9-digit book number in the Search Support field, and then click **Go**.

   The system displays the Product Documentation Search Results page.
4. Scroll down to find the latest issue number, and then click the book title that is to the right of the latest issue number.
5. On the next page, scroll down and click one of the following options:

   - **PDF Format** to download the book in regular PDF format.
   - **ZIP Format** to download the book in zipped PDF format.

European Union standards

Avaya declares that the DEFINITY equipment specified in this document bearing the "CE" mark conforms to the European Union Electromagnetic Compatibility Directives.

The "CE" (Conformité Européenne) mark indicates conformance to the European Union Electromagnetic Compatibility Directive (89/336/EEC), Low Voltage Directive (73/23/ECC), and Telecommunication Terminal Equipment (TTE) Directive (91/263/EEC) and with i-CTR3 Basic Rate Interface (BRI) and i-CTR4 Primary Rate Interface (PRI) as applicable.

Standards compliance

The equipment presented in this document complies with the following (as appropriate):

- ITU-T (Formerly CCITT)
- ECMA
- ETSI
- IPNS
- DPNSS
- National ISDN-1
- National ISDN-2
- ISO-9000
- ANSI
- FCC Part 15 and Part 68
- EN55022
- EN50081
- EN50082
- CISPR22
- Australia AS3548 (AS/NZ3548)
- Australia AS3260
- IEC 825
- IEC950
- UL 1459
- UL 1950
- CSA C222 Number 225
- TS001

Conventions

This section describes the conventions that we use in this book.

General

We show commands and screens from the newest Avaya system and see the most current books. You must substitute the appropriate commands for your system and see the books that you have available.

Physical dimensions

- All physical dimensions in this book are in English units followed by metric units in parentheses.
- Wire gauge measurements are in AWG followed by the diameter in millimeters in parentheses.

Typography

This section describes the typographical conventions for commands, keys, user input, system output, and field names.

Commands

- Commands are in **bold** type.

  Example

  Type **change-switch-time-zone** and press **Enter**.
- Command variables are in ***bold italic*** type when they are part of what you must type, and in *plain italic* type when they are not part of what you must type.

  Example

  Type **ch ma machine_name**, where *machine_name* is the name of the call delivery machine.
- Command options are in **bold** type inside square brackets.

  Example

  At the DOS prompt, type **copybcf [-F34]**.

Keys

- The names of keys are in **bold sans serif** type.

  Example

  Use the **Down Arrow** key to scroll through the fields.
- When you must press and hold a key and then press a second or third key, we separate the names of the keys are separated with a plus sign (+).

  Example

  Press **ALT+D**.

- When you must press two or more keys in sequence, we separate the names of the keys are separated with a space.

  Example

  Press **Escape J**.

- When you must press a function key, we provide the function of the key in parentheses after the name of the key.

  Example

  Press **F3** (Save).

User input

- User input is in **bold** type, whether you must type the input, select the input from a menu, or click a button or similar element on a screen or a Web page.

  Examples

  — Type **exit**, and then press **Enter**.

  — On the **File** menu, click **Save**.

  — On the Network Gateway page, click **Configure** > **Hardware**.

System output and field names

- System output and field names on the screen are in `monospaced` type.

  Examples

  — The system displays the following message:

  ```
  The installation is in progress.
  ```

  — Type **y** in the `Message Transfer?` field.

Safety labels and security alert labels

Observe all caution, warning, and danger statements to help prevent loss of service, equipment damage, personal injury, and security problems. This book uses the following safety labels and security alert labels:

CAUTION:
A caution statement calls attention to a situation that can result in harm to software, loss of data, or an interruption in service.

WARNING:
A warning statement calls attention to a situation that can result in harm to hardware or equipment.

Use an ESD warning to call attention to situations that can result in ESD damage to electronic components.

DANGER:
A danger statement calls attention to a situation that can result in harm to personnel.

A security alert calls attention to a situation that can increase the potential for unauthorized use of a telecommunications system.

Safety precautions

DANGER:
Electrical current from power, telephone, and communication cables is hazardous.

To avoid a shock hazard:

Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.

Connect all power cords to a properly wired and grounded electrical outlet.

Connect to properly wired outlets any equipment that will be attached to this product.

When possible, use one hand only to connect or disconnect signal cables.

Never turn on any equipment when there is evidence of fire, water, or structural damage.

Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.

Connect and disconnect cables as described in Table 1, Connecting and disconnecting cables, on page 13 when installing, moving, or opening covers on this product or attached devices.

Table 1: Connecting and disconnecting cables

To connect:		To disconnect:	
1	Turn everything off.	1	Turn everything off.
2	Attach all cables to devices.	2	Remove power cords from outlet.
3	Attach signal cables to connectors.	3	Remove signal cables from connectors.
4	Attach power cords to outlet.	4	Remove all cables from devices.
5	Turn device ON.		

DANGER:
Some laser products contain an embedded Class 3A or Class 3B laser diode. Note the following:

Laser radiation when open. Do not stare into the beam, do not view directly with optical instruments, and avoid direct exposure to the beam.

CAUTION:
When laser products (such as CD-ROMs, DVD drives, fiber optic devices, or transmitters) are installed, note the following:

Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.

Use of controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure.

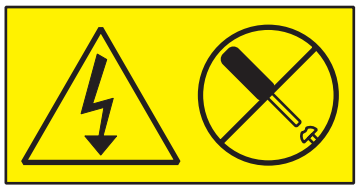
CAUTION:
Use safe practices when lifting.

For items heavier than 37 lb (18 kg), two people are required.
For items heavier than 70.5 lb (32 kg), three people are required.
For items heavier than 121.2 lb (55 kg), four people are required.

CAUTION:
The power control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.

CAUTION:
If you install a strain-relief bracket option over the end of the power cord that is connected to the device, you must connect the other end of the power cord to an easily accessible power source.

CAUTION:
Never remove the cover on a power supply or any part that has the following label attached.

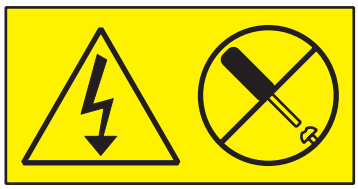

lbmswarn LAO 073003

Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

CAUTION:
Do not place any object weighing more than 180 lb (82 kg) on top of rack-mounted devices.

CAUTION:
Overloading a branch circuit is potentially a fire hazard and a shock hazard under certain conditions. To avoid these hazards, ensure that your system electrical requirements do not exceed branch circuit protection requirements. See the information that is provided with your RSA for electrical specifications.

CAUTION:
Hazardous voltage, current, and energy levels might be present. Only a qualified service technician is authorized to remove the covers where the following label is attached.


lbmswarn LAO 073003

CAUTION:
Make sure that the rack is secured properly to avoid tipping when the server unit is extended.

CAUTION:
Some accessory or option board outputs exceed Class 2 or limited power source limits and must be installed with appropriate interconnecting cabling in accordance with the national electric code.

CAUTION:
To reduce the risk of electric shock or energy hazards:

This equipment must be installed by trained service personnel in a restricted-access location, as defined by the NEC and IEC 60950, Third Edition, The Standard for Safety of Information Technology Equipment.

Connect the equipment to a reliably grounded safety extra low voltage (SELV) source. An SELV source is a secondary circuit that is designed so that normal and single fault conditions do not cause the voltages to exceed a safe level (60 volts direct current).

The branch circuit overcurrent protection must be rated at a minimum of 5 amperes to a maximum of 15 amperes.

Use 14 American Wire Gauge (AWG) or 2.5 mm2 copper conductor only, not exceeding three meters in length.

Torque the wiring-terminal screws to 12 inch-pounds (1.4 newton-meters).

CAUTION:
The power-control button on the device does not turn off the electrical current supplied to the device. The device might also have more than one connection to dc power. To remove all electrical current from the device, ensure that all connections to dc power are disconnected at the dc power input terminals.

Trademarks

Trademarks and Service Marks

The following are trademarks or registered trademarks of Avaya:

- AUDIX®
- Cajun®
- Callvisor®
- Callmaster®
- CentreVu™
- CONVERSANT®
- DEFINITY®
- DIMENSION®
- INTUITY™

- MERLIN®
- MultiVantage™
- Softconsole™
- TransTalk®
- VOICE POWER®

The following are trademarks or registered trademarks of Lucent Technologies:

- 5ESS™, 4ESS™

The following are trademarks or registered trademarks of AT&T:

- ACCUNET®
- DATAPHONE®
- MEGACOM®
- MULTIQUEST®
- TELESEER®

The following are trademarks or registered trademarks of other companies:

- Acrobat® (registered trademark of Adobe Systems Incorporated)
- Ascend® (registered trademark of Ascend, Inc.)
- Audichron® (registered trademark of Audichron Company)
- MS-DOS® (registered trademark of the Microsoft Corporation)
- MicroChannel® (registered trademark of IBM Systems)
- Microsoft® (registered trademark of Microsoft Corporation)
- MULTIQUEST® (registered trademark of Telecommunications Service)
- NetMeeting® (registered trademark of Microsoft Corporation)
- PagePac® (trademark of the Dracon Division of the Harris Corporation)
- PictureTel® (registered trademark of PictureTel Corporation)
- ProShare® (registered trademark of Intel Corporation)
- UNIX® (trademark of the Novell Corporation)
- Zydacron (registration pending for Zydacron Corporation)

Technical assistance

Avaya provides the following resources for technical assistance.

Within the United States

For help with:

- Feature administration and system applications, call the Avaya DEFINITY Helpline at 1-800-225-7585
- Maintenance and repair, call the Avaya National Customer Care Support Line at 1-800-242-2121
- Toll fraud, call Avaya Toll Fraud Intervention at 1-800-643-2353

International

For all international resources, contact your local Avaya authorized dealer for additional help.

Sending us comments

Avaya welcomes your comments about this book. To reach us by:

- Mail, send your comments to:

  Avaya Inc.

  Product Documentation Group

  Room B3-H13

  1300 W. 120 Ave.

  Westminster, CO 80234 USA

- E-mail, send your comments to:

  document@avaya.com

- Fax, send your comments to:

  1-303-538-1741

Be sure that you mention the name and number of this book, *Avaya Remote Supervisor Adapter User Guide*, 555-245-702.

Using the Avaya Remote Supervisor Adapter

Overview

The Avaya Remote Supervisor Adapter (RSA) is installed in PCI-X slot 1 of the S8500 Media Server. Administration of the RSA is accomplished through the Advanced System Management (ASM) Web interface using a browser.

The following are highlights of the features of the RSA:

- Monitors the health of the Avaya S8500 Media Server
- Timed stamped event logs
- Remote access via LAN or serial modem
- Point-to-point protocol (PPP) support
- Simple Network Management Protocol (SNMP) support
- Notification and alerts sent via SNMP, modem, e-mail, or numeric pager
- Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) support
- Ability to remotely power on or off the S8500 Media Server
- Remote firmware upgrades
- Web based access using the Advanced System Management Interface

Web browser requirements

You can use the following Web browsers to remotely access the RSA:

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

NOTE:
When using the ASM Web Interface, monitor resolution should be set to 800 x 600 pixels and 256 colors, and double-byte character set (DBCS) languages are not supported.

NOTE:
The values in all windows are examples. Your settings will be different.

NOTE:
Disable the Sun Java Virtual machine.

Connecting and logging in to the RSA

To access the RSA remotely using the ASM Web interface, you must log in to the adapter.

To connect and log in to the RSA:

6 Connect the services laptop to the Ethernet port on the RSA using a crossover cable.

7 Open an internet browser window.

8 In the **Address** field, type **192.11.13.6** and press **Enter**.

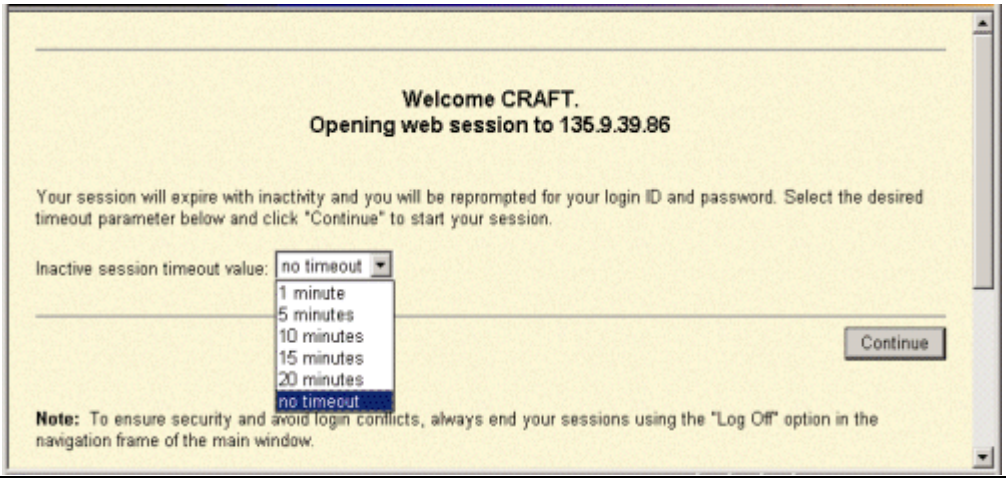
The Enter Network Password window appears (see Figure 1, Network password window, on page 20).

Figure 1: Network password window

9 Type the default login **craft** and default password **passw0rd** (with a zero).

The RSA welcome screen appears (see Figure 2, Log into the RSA, on page 20).

Figure 2: Log into the RSA



10 In the **Inactive session timeout value** field, select **no timeout**. The **no timeout** value allows 60 minutes of use before disconnecting.

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

NOTE:
If the session times out unexpectedly, click **Start New Session** and **Refresh**.

WARNING:
Executing the **Restore ASM Defaults** option in the navigation pane removes the Avaya defaults. Avaya defaults can be restored manually using the information found in the Avaya RSA Defaults section or by restoring the Avaya default file. The Avaya default file can be found at http://support.avaya.com or on the Communication Manager 2.0 CD for Linux Servers and Gateways. For instructions on restoring the default file, see Restoring and modifying the ASM configuration.

ASM navigation

ASM navigation pane layout

The ASM screen is divided into a navigation pane and a display pane (see Figure 3, Navagation pane, on page 21).

Figure 3: Navagation pane

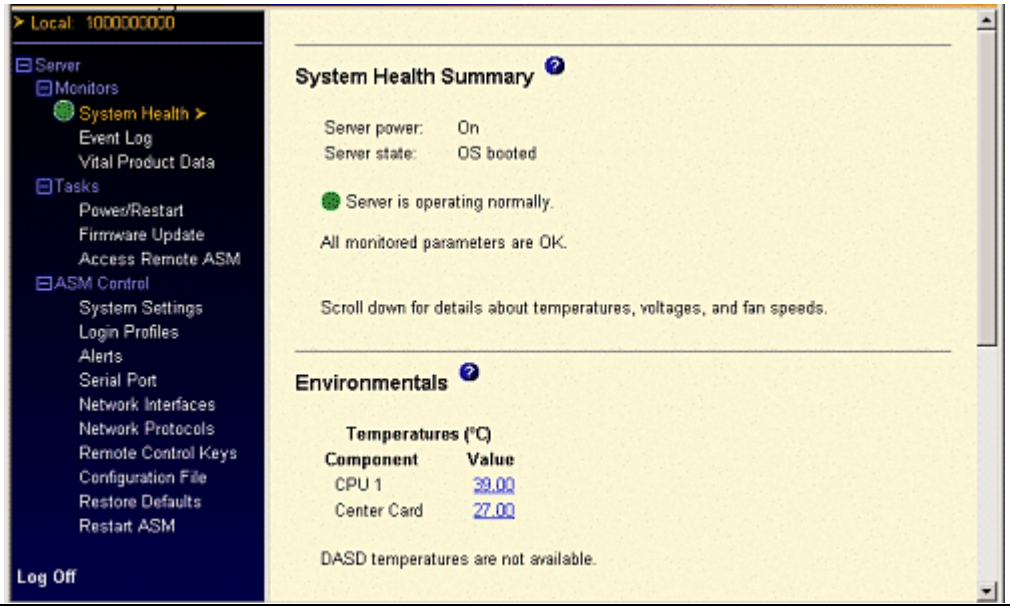


Table 2, Available actions, on page 22 outlines the actions available in the navigation pane.

Table 2: Available actions ***1 of 3***

Link	Action	Description
System Health	View health of the S8500 Media Server and the users logged into the RSA.	View the power, temperature, voltage, and fan status of the S8500 Media Server. You also can view the users logged into the RSA.
Event Log	View S8500 event logs.	Event logs contain S8500 information pertaining to Power On Self Test (POST), remote access attempts, and dial-out events. Events are time stamped. Some of the events generate an alert if configured on the Alerts page.
Vital Product Data (VPD)	View the VPD for the S8500 server.	When the server starts, the RSA collects system data, basic input/output system (BIOS) information, and the server component VPD, and stores it in nonvolatile memory.
Power/Restart	Remotely power on/off or restart the S8500 Media Server.	The RSA provides full power on, power off, and restart capability for the S8500 Media Server.
Firmware Update	Update the firmware on the RSA.	The firmware on the RSA can be updated. The firmware update can be obtained from http:\\support.avaya.com.
Access Remote ASM	Not used in the S8500 Media Server configuration.	
System Settings	View and configure system settings for the RSA.	This screen is divided into three sections: • **ASM Information**: S8500 Product ID, ID number, contact, and location information. • **Server Timeouts**: Power off delay. • **ASM Date and Time**: Set the date, time, GMT offset, and daylight savings time.
Login Profiles	Configure the RSA login files	View, configure, or change individual login profiles. Up to 12 login profiles can be defined.

1 of 3

Table 2: Available actions ***2 of 3***

Link	Action	Description
Alerts	View and configure local events, alerts and define alert recipients.	This screen is divided into five sections: • **Remote Alert Recipients**: Define name, notification method, number, PIN, e-mail address, and PPP login ID and password. • **Alert Forwarding**: Not used in the S8500 Media Server configuration. • **Global Remote Alert Settings**: Defines the number of times an alert retries and the delay time between retries. • **Monitored Alerts**: Defines the type of alerts within categories that will be sent to an remote alarm recipient. • **Monitored Local Events**: Defines the type of monitored events that will be sent to a local alarm recipient.
Serial Port	Configure the serial port and modem settings.	Use to configure the serial port and modem settings. The serial port on the RSA must be dedicated to the RSA.
Network Interfaces	Configure the network interfaces used with RSA.	This screen is divided into two sections: • **Ethernet**: Define if Ethernet is enabled or disabled and if DHCP or static IP addressing will be used. • **PPP over Serial Port**: Define if PPP will be used over the serial port, local IP address, remote IP address, subnet mask, and authentication.
Network Protocols	Configure the network protocols used with the RSA.	This screen is divided into three sections: • **Simple Network Management Protocol (SNMP)**: Enable or disable SNMP agents and traps, set community names, host name or IP address. • **Domain Name System (DNS)**: Enable or disable DNS, set IP address of the DNS, and configure the host table. • **Simple Mail Transfer Protocol (SMTP)**: Define the server host name or IP address.
Remote Control Keys	Not used in the S8500 Media Server configuration.	
Configuration File	Backup, modify, and restore ASM configuration.	Backup and restore the ASM configuration using the Configuration File selection.

2 of 3

Table 2: Available actions ***3 of 3***

Link	Action	Description
Restore Defaults	Restore the RSA to the factory default configuration.	Use to restore the RSA configuration information to factory defaults. When this option is selected: • Your current session terminates. • Your login and password are lost. • All current configuration information is erased. • All Avaya default settings are erased.
Restart ASM	Restart the RSA board.	Use to restart the RSA board.
Log Off	Log off the RSA.	Use to terminate your RSA connection.

3 of 3

ASM control

This section outlines the procedures needed to configure the ASM. You use the links under **ASM Control** in the navigation pane to configure the RSA.

Viewing the configuration summary

You may view the entire configuration of the RSA by clicking **View Configuration Summary** in the upper right hand corner of all entries under the **ASM Control** heading except for the **Configuration File**, **Restore Defaults**, and **Restart ASM** windows.

System settings

From the **System Settings** window, you can:

- Set ASM information
- Set server timeouts
- Set ASM date and time

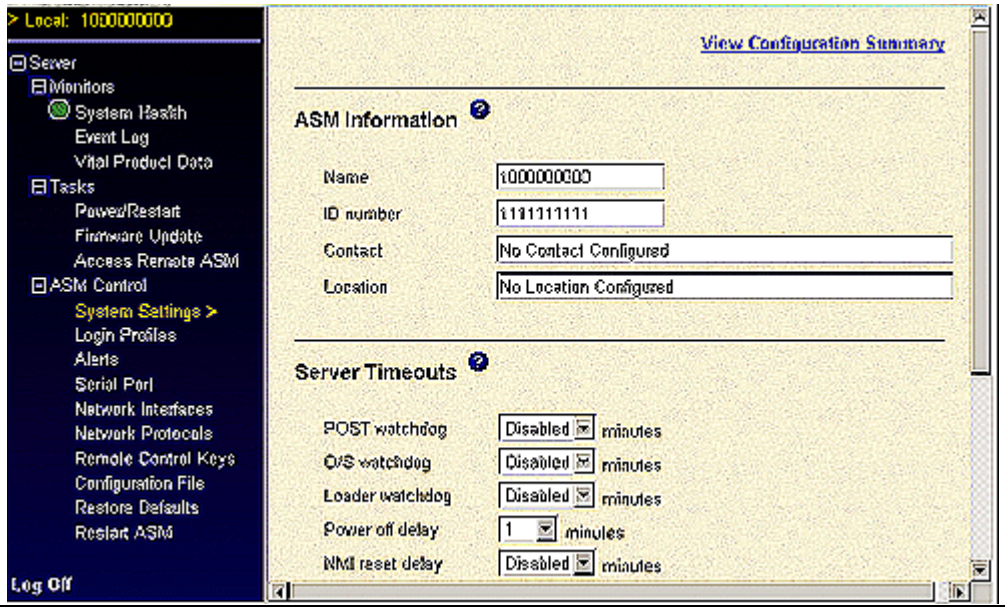
Setting system information

To set system information:

- In the navigation pane, select **System Settings** under the **ASM Control** heading.

  The System Settings window appears (see Figure 4, System settings, on page 25).

Figure 4: System settings



NOTE:
The RSA is shipped with recommended Avaya defaults. With write permissions on your login ID, it is possible to change any default to customize your server. To save any changes made to this section, scroll to the bottom of the page and click **Save**.

Setting ASM information

To set ASM information:

1. In the navigation pane, select **System Settings** under the **ASM Control** heading.

   The System Settings window appears.

2. **Name [default: 1000000000]**: This required field must contain the product ID associated with the S8500 Media Server in this location. Avaya Services uses the product ID to identify the RSA and associated S8500 Media Server.

3. **ID Number [default: 100000000]**: Type an ID number that will be used to identify the S8500 Media server. This information will be part of the SNMP trap.

4. **Contact [default: no contact configured]**: An optional field that contains the name of the person responsible for this server at this location. You can enter a maximum of 47 characters in this field.

5. **Location [default: no location configured]**: An optional field that contains the address of the location where the server resides. You can enter a maximum of 47 characters in this field.

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

Setting server time-outs

To set server time-outs:

1. **I**n the navigation pane, select **System Settings** under the **ASM Control** heading.

   The System Settings window appears.

2. **POST Watchdog [default: Enabled, 5 minutes**]: Use this field to specify the number of minutes that the RSA will wait for the S8500 Media Server to complete a power-on self-test (POST). If the S8500 Media Server fails to complete a POST within the selected time period, the RSA generates a POST time-out and reboots the S8500 Media Server. At that point the POST watchdog is disabled until:

   - The operating system is shut down and the server is power cycled.
   - The operating system starts and the ASM device drivers successfully load.

   To set the POST watchdog, select a value from the drop-down menu. To turn this option off, select **Disabled**.

3. **O/S Watchdog [default: Enabled, 2.5 minutes]**: Use this field to specify the number of minutes between checks of the operating system by the RSA. If the operating system fails to respond to a check, the RSA generates an O/S time-out alert and reboots the S8500 Media Server. The O/S alert is generated only if the **O/S Timeout** check box has been selected in the **Monitored Alert** section of the **Alerts** page (see Alerts for more information). After the S8500 Media Server is restarted, the O/S Watchdog is disabled until the S8500 is shut down and power cycled.

   To set the O/S Watchdog, select a value from the drop-down menu. To turn this option off, select **Disabled**.

4. **Loader Watchdog [default: Enabled, 5 minutes]**: Use this field to specify the number of minutes that the RSA waits between completion of POST and the start of the operating system. If the value that was selected for the Loader Watchdog is exceeded, the RSA generates a Loader time-out alert and restarts the S8500 Media Server. The Loader Watchdog alert is generated only if the Loader Time-out check box has been selected in the Remote Alert section of the Alerts page (see Alerts for more information). At this point, the Loader Watchdog is disabled until:

   - The operating system shuts down and the server power cycles.
   - The operating system starts and the ASM device drivers successfully load.

   To set the Loader Watchdog, select a value from the drop-down menu.To turn this option off, select **Disabled**.

5. **Power Off Delay [default: Enabled, 0.5 minutes]**: Use this field to set the amount of time in one minute increments that the S8500 Media Server delays shutting down to ensure that the shutdown of the operating system has completed.

   NOTE:
   If the power off selected value is less then 45 seconds, the RSA device drivers automatically set the value to 45 seconds when they load. The value can be decreased once the S8500 Media Server has started but the RSA device driver resets the value to be 45 seconds the next time the server restarts. The RSA device drivers do not change a value that is 45 seconds or greater.

   To set the Power Off Delay, select a value from the drop down menu.

6 **NMI Reset Delay [default: Disabled]**: Use this field to specify the time in minutes that the RSA waits to restart the S8500 Media Server after a nonmaskable interrupt (NMI) generates. A NMI can be triggered by:

- A critical error such as a hardware fault.
- A parity error in the memory subsystem.

To set the NMI Reset Delay, select a value from the drop-down menu. To turn this option off, select **Disabled**.

7 Scroll to the bottom of the page and slick **Save**.

Setting ASM date and time

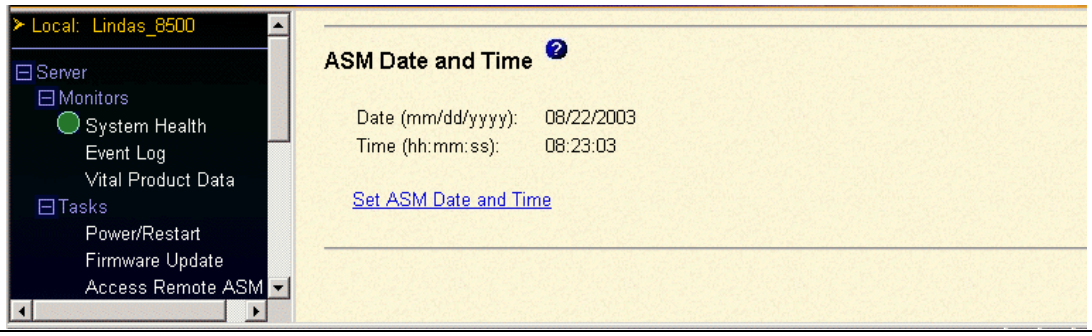
Alerts that are sent from the RSA are time stamped using the RSA internal clock. The RSA internal clock uses Greenwich Mean Time (GMT) and Daylight Saving Time (DST) to enable administrators to manage servers that reside in different time zones.

To set the date and time:

1 In the navigation pane, select **System Settings** under the **ASM Control** heading.

The ASM Date and Time window appears (see Figure 5, ASM date and time, on page 27).

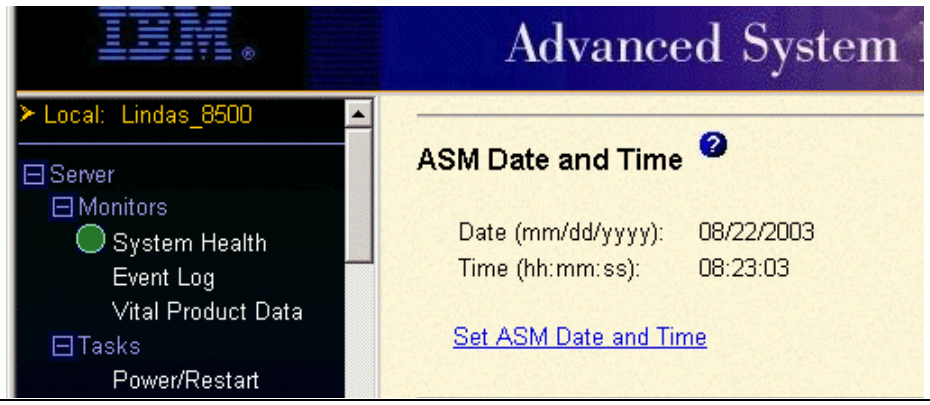
Figure 5: ASM date and time



2 Scroll down to the **ASM Date and Time** section and click **Set ASM Date and Time**.

The ASM Date and Time window opens (see Figure 6, ASM Date and Time, on page 27).

Figure 6: ASM Date and Time



3 **Date**: Type the current month, day, and year.

4 **Time**: Type the current hour (hh), minutes (mm), and seconds (ss). The hour must be a value from 00 to 23. The minutes and seconds must be a value from 00 to 59.

5 **GMT offset [default: +0:00]**: Type the number of the offset in hours that corresponds to the time zone where the server is located.

6 **Automatically adjust for daylight saving changes (DST) [default: not checked/Disabled]**: Check if the location where the server resides uses DST.

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

8 The main **System Settings** window opens. Scroll to the bottom of the screen and click **Save**.

Login profiles

From the **Login Profiles** window, you can:

- View, configure, or change individual login profiles.
- Configure modem and dial-in settings.

Each link in the Login ID column contains the configured login ID for that particular profile. If you have not configured a profile, the name of the link shows "not used."

Creating a login profile

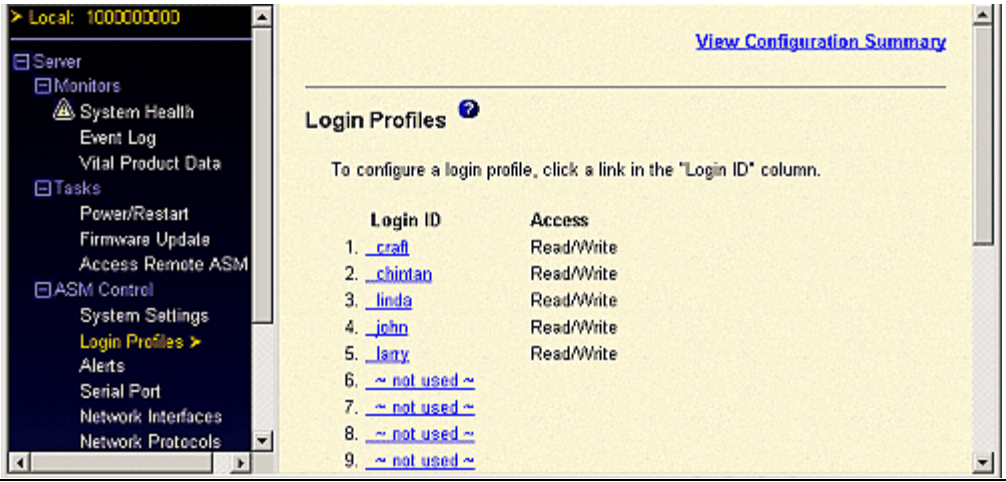
NOTE:
You can create up to 12 login profiles.

To create a login profile:

1 In the navigation pane, select **Login Profiles** under the **ASM Control** heading.

The Login Profiles window appears (see Figure 7, Login profiles, on page 28).

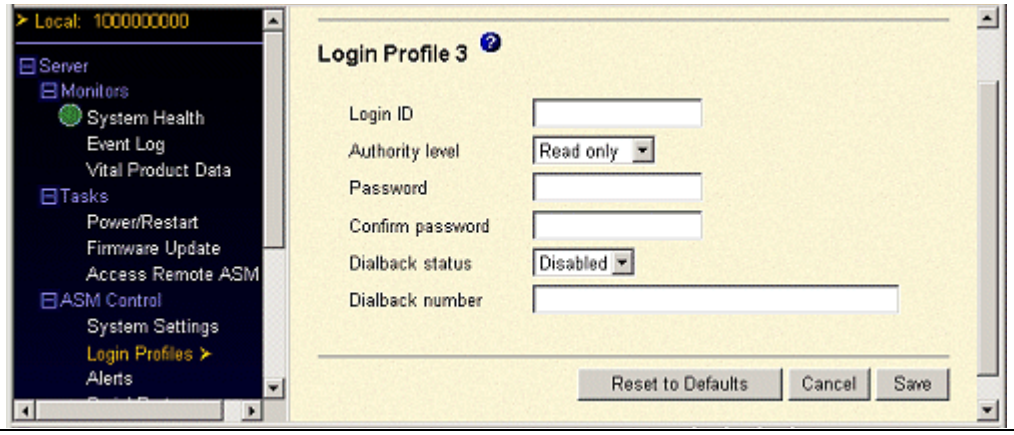
Figure 7: Login profiles



2 Click **not used** associated with an unused login profile link.

A login profile window opens (see Figure 8, Login profile, on page 29).

Figure 8: Login profile



3 In the **Login ID** field **[default: craft]**: Type a unique login ID consisting of a maximum of 15 characters in length. Valid characters include letter, digits, periods, and underscores.

4 In the **Authority level** field **[default: Read/Write]**: Assign permissions of read and write access or read access only.

- **Read only**: Gives the user the ability to view a window. Read only users do not have the permission to perform file transfers, power and restart actions, or remote control functions.
- **Read/Write**: Gives the user the ability to perform all available actions contained in the RSA Web interface.

5 In the **Password** field **[default: passw0rd]**: Assign a password of at least 5 characters made up of both alphabetic and numeric characters, one of which must be a non-alphabetic character. Null or empty passwords are accepted.

6 In the **Confirm password** field: Type the password again.

NOTE:
The **Dialback status** and **Dialback number** fields are not used.

7 Click **Save**.

The Login Profiles window appears.

8 Scroll down and click **Save** to save the settings.

WARNING:
An Avaya default login profile **craft** was created to allow first time access. The default password associated with **craft** is **passw0rd** (the 0 is a zero). This password should be changed during the initial setup of the RSA to avoid potential security exposure. If the **Restore Default** option was selected in the navigation pane, the default login will be **USERID** with the password of **PASSW0RD** (the 0 is a zero).

Setting the global login settings

This procedure allows you to enable your modem to dial out to the remote login profile.

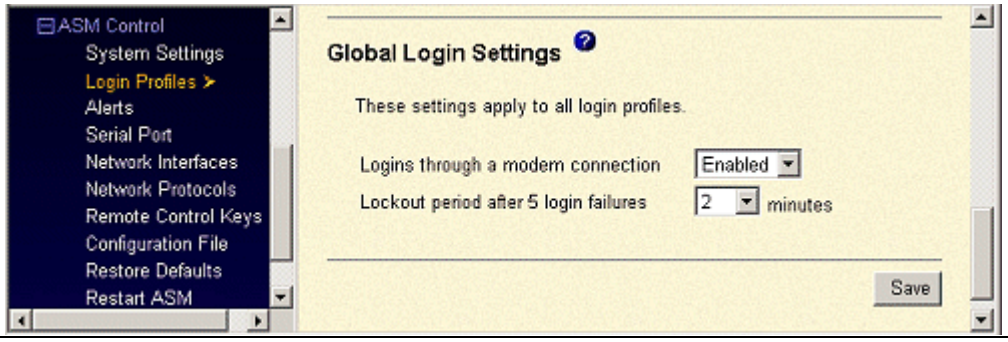
> **NOTE:**
> The global login settings apply to all login profiles.

To set the Global Login Settings:

1. In the navigation pane, select **Login Profiles** under the **ASM Control** heading.

   The Global Login Settings window appears (see Figure 9, Global login settings, on page 30).

Figure 9: Global login settings



2. Scroll down to the **Global Login Settings** section of the window.
3. In the **Logins through a modem connection** field **[default: Enabled]**: Select **Enabled** to log in through a modem connection.
4. In the **Lockout period after 5 login failures** field **[default: 2 minutes]**: Select the time in minutes that someone would be locked out after attempting to login to the RSA five times.
5. Click **Save** to save the settings.

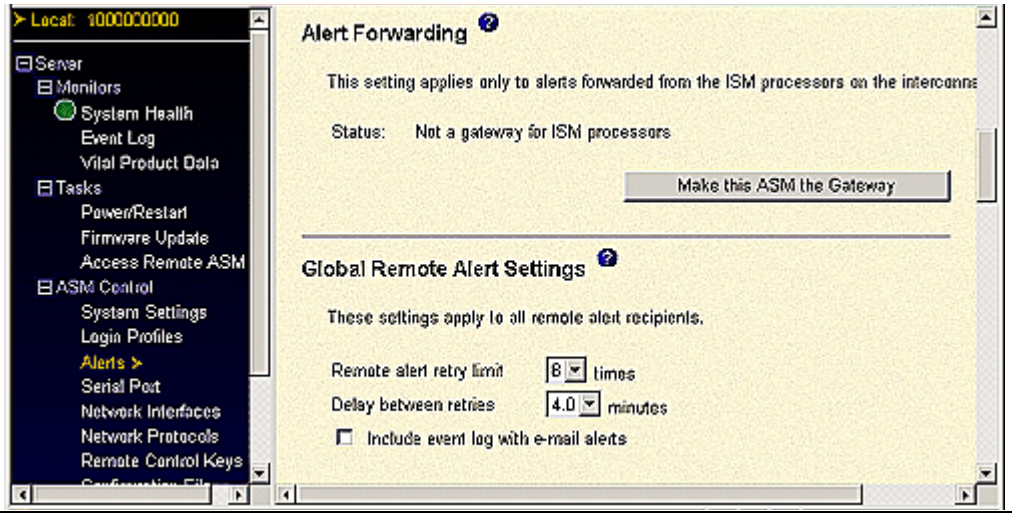
Alerts

From the **Alerts** window, you can:

- Configure alert recipients.
- Set the number of remote alert attempt.
- Select the delay between alerts.
- Define incidents that trigger remote and local alerts.

Use the **Alert** selection under **ASM Control** (see Figure 10, Alerts, on page 31).

Figure 10: Alerts



NOTE:
Please read the following notes before proceeding.

- Before an SNMP Agent or an SNMP Trap alarm can be generated they must be enabled. Enable the SNMP Agent and the SNMP Trap using the **Simple Network Management Protocol** configuration screens found under the **Network Protocols** link.
- The **Serial Port** under **ASM Control** must be configured before an alert can be generated over the serial port
- You cannot separate the alert types that will be sent to alert recipients. All configured alert recipients receive every alert that is selected.
- To send alerts to an Avaya service center over modem, select **IBM Director over Modem** from the **Notification Method** field.
- To send alerts to an Avaya service center over LAN, select **SNMP over LAN** from the **Notification Method** field.

Configuring a remote alert recipient

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

To configure or view a remote alert recipient:

- Select **Alerts** in the navigation pane.

  The Remote Alert Recipient screen displays the name, selected notification method, and status of enabled or disabled. You can configure a maximum of 12 alert recipients.

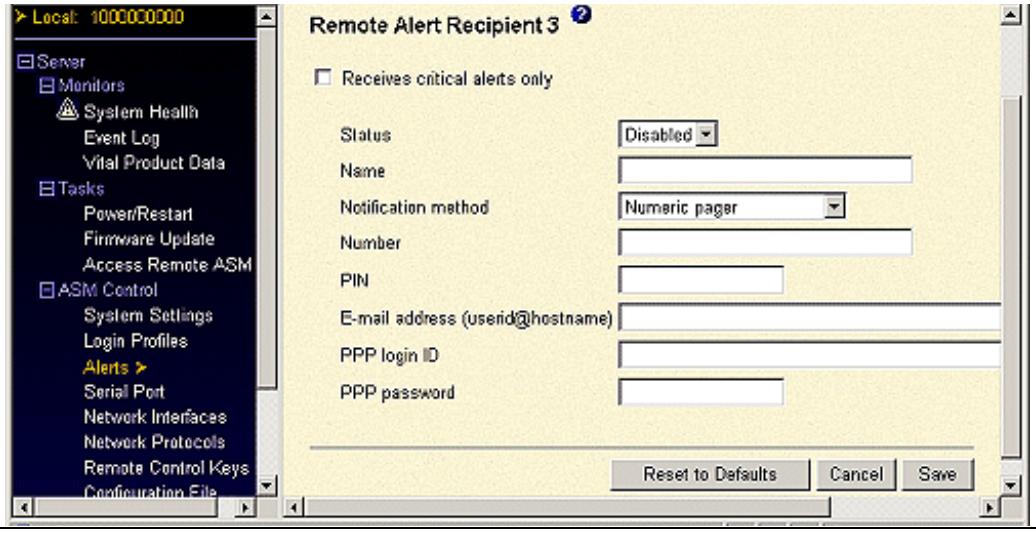
Adding a remote alert recipient

To add a remote alert recipient:

1. In the **Remote Alert Recipients** section, click **not used** in an unused position of the next available slot.

   A new screen opens with the following configuration fields (see Figure 11, Remote alert recipient window, on page 32):

Figure 11: Remote alert recipient window



- **Receives Critical Alerts Only**: If this box is checked, the alert recipient receives notification only for critical alerts. To view what constitutes a critical alert, select **Alerts** in the navigation pane and scroll down to **Monitored Alerts**.
- **Status**: Click on the drop-down menu and select **Enabled** to activate this remote alert recipient.
- **Name**: Type the name of the alert recipient.
- **Notification Method**: Use the drop-down menu to select the notification method that will be used to reach the recipient. Methods include:
  - Numeric Pager
  - Alphanumeric pager
  - IBM Director over Modem: In the case where an Avaya service contract is in place or the system is under warranty, this option could be used to report alarms to an Avaya service center.
  - IBM Director over LAN - Avaya recommends not using this option.
  - SNMP over LAN: In the case where an Avaya service contract is in place or the system is under warranty, this option could be used to report alarms to an Avaya services center.
  - E-mail over LAN - Avaya recommends not using this option.
  - SNMP over PPP
  - E-mail over PPP - Avaya recommends not using this option.

  NOTE:
  IBM Director over Modem and **SNMP over LAN** are the methods supported by Avaya services.

- **Number**: Type a telephone number, IP address, or host name if one of the following selections were made in the **Notification Method** field:
  - **Numeric pager**: Type the telephone number followed by a comma, and then personal identification number (PIN).
  - **Alphanumeric pager**: Only a telephone number is required for an alphanumeric pager. The PIN number is a separate entry that is entered in the PIN field.
  - IBM Director over modem: In the case where an Avaya service contract is in place or the system is under warranty, this field may contain the number for an Avaya service center.
  - SNMP over PPP
  - E-mail over PPP
- **PIN**: If an alphanumeric pager was selected as the form of notification, enter a PIN.
- **E-Mail Address**: If e-mail over LAN or e-mail over PPP was selected as the form of notification, enter an e-mail address.

NOTE:
For **E-mail over LAN** or **E-mail over PPP** notification to work properly, type the host name or IP address for the SMTP in Network Protocols. For more information on configuring the SMTP refer to Network protocols.

2. Click **Save** to save any additions or modifications to the **Remote Alert Recipients** fields.
3. Click **Generate Test Alert** to generate a test alarm to all configured remote alarm recipients.

Alert fowarding

This option does not apply in a S8500 Media Server configuration.

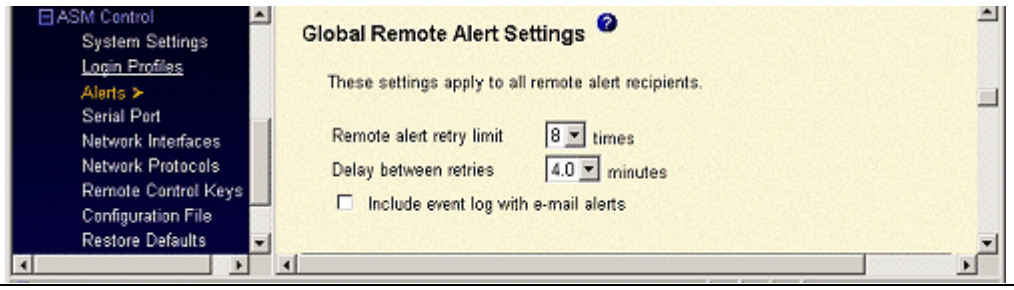
Configuring global remote alert settings

The Global Remote Alert Settings fields define the number of times an alert retries and the delay time between retries. These global settings effect every alert recipient.

To configure the global remote alert settings:

1. In the navigation pane, select **Alerts** under the **ASM Control** heading.
2. Scroll down to the **Global Remote Alert Settings** section (see Figure 12, Global remote alert settings, on page 33).

Figure 12: Global remote alert settings



3 In the **Remote alert retry limit** field **[default: 8 times]**: From the drop-down menu, select the number of additional times that the RSA tries to send an alert to a remote recipient.

4 In the **Delay between retries** field **[default: 4 minutes]**: From the drop-down menu, select the delay time between alert notification attempts to a recipient.

5 In the **Include event log with e-mail alerts** field **[default: Disabled]**: Select the box if:

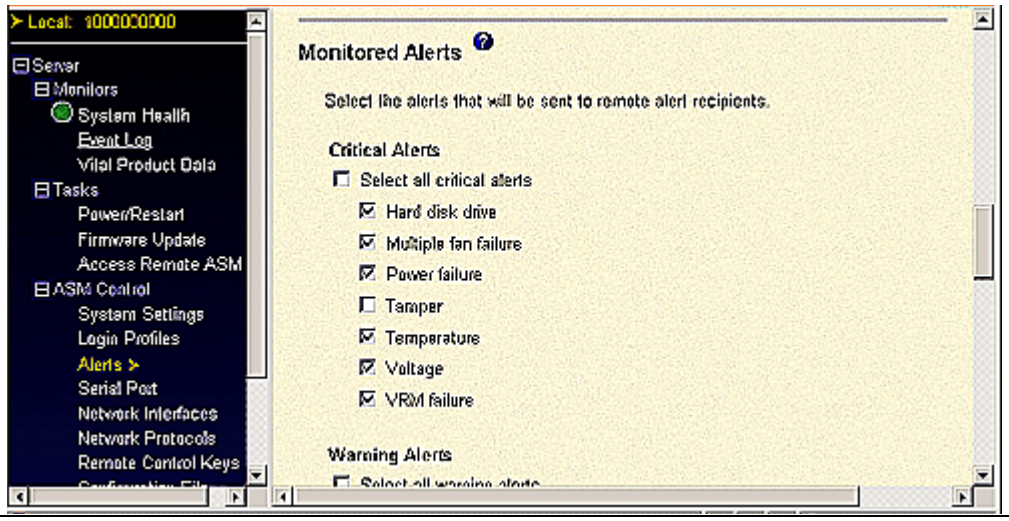
- You wish to attach a copy of the local event log to e-mail alert notifications
- If at least one alert recipient has e-mail or LAN or e-mail over PPP selected as their means of alert notification.

6 To save any changes to the global remote alert settings, click **Save**.

Customizing monitored alerts

You can customize the types of alerts that will be associated with critical, warning, and system level severities. All alerts are time stamped and stored in the RSA event log. You must select the box next to the type of alert you wish to receive notification on. All alerts have a default setting of enabled**.** See Figure 13, Monitored alerts, on page 34.

Figure 13: Monitored alerts



To customize a monitored alert:

1 In the navigation pane, select **Alerts** under the **ASM Control** heading.

2 Scroll down to the desired alert section and make your changes.

Critical alerts

Critical alerts are generated when one or more critical components are no longer functioning. See Table 3, Critical alerts, on page 35 for an explanation of critical alerts.

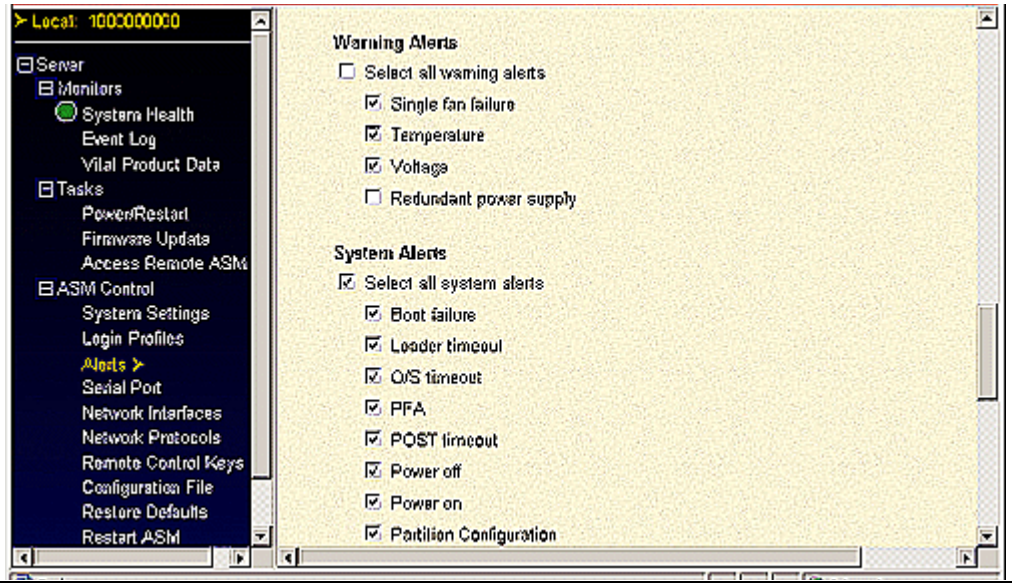
Table 3: Critical alerts

Alphanumeric Pager Code	Event	Action
00	Temperature irregularity	**[default: Enabled]:** Generates an alert if any of the monitored temperatures fall outside the critical threshold values. If a critical temperature setting is detected, the S8500 Media Server shuts down. This shutdown happens even if this field is **not** selected for alert notification. To view the threshold values associated with the temperature readings, select **System Health** in the navigation pane. Under **Environmentals, Temperature**, click **Value**. A window opens that shows the warning reset, warning, soft shutdown, and hard shutdown thresholds for temperatures associated with the selected component.
01	Voltage irregularity	**[default: Enabled]:** Generates an alert if voltages for any of the monitored power supplies fall outside their specified operating ranges. If a critical voltage condition is detected, the S8500 Media Server shuts down. The shutdown happens even if this field is **not** selected to generate an alert notification. To view the voltage operating setting, select **System Health** on the navagation pane. Under **Environmentals, Voltages**, click **Value.** A window opens that shows the warning reset, warning, soft shutdown, and hard shutdown thresholds for voltages associated with the selected components.
02	Tamper	**[default: Disabled]:** Not used in the S8500 Media Server configuration.
03	Multiple fan failure	**[default: Enabled]:** Generates an alert if two or more cooling fans fail.
04	Power failure	**[default: Enabled]: G**enerates an alert if the power unit on the S8500 Media Server fails.
05	Hard disk drive failure	**[default: Enabled]:** Generates an alert if the S8500 hard disk fails.
06	VRM failure	**[default: Enabled]:** Generates an alert if one or more voltage regulator modules (VRMs) fail.

Warning alerts

Warning alerts are generated for events that may progress into a critical level. See Figure 14, Warning and System Alerts, on page 36.

Figure 14: Warning and System Alerts



See Table 4, Warning alerts, on page 36 for an explanation of warning alerts.

Table 4: Warning alerts

Alphanumeric Pager Code	Event	Action
10	Redundant power supply failure	**[default: Disabled]:** Not used in the S8500 Media Server configuration.
11	Single fan failure	**[default: Enabled]:** Generates an alert if one fan fails.
12	Temperature irregularity	**[default: Enabled]:** Generates an alert if any monitored temperature readings are outside the warning threshold. The S8500 Media Server remains in service. To view the threshold values associated with the temperature readings, select **System Health** in the navigation pane. Under **Environmentals, Temperature,** click **Value**. A window opens that shows the warning reset, warning, soft shutdown, and hard shutdown thresholds for temperatures associated with the selected component.
13	Voltage irregularity	**[default: Enabled]:** Generates an alert if any monitored voltages are outside the warning threshold values. The S8500 Media Server remains in service. To view the voltage operating setting, select **System Health** in the navigation pane. Under **Environmentals, Voltages**, click **Value.** A window opens that shows the warning reset, warning, soft shutdown, and hard shutdown thresholds for voltages associated with the selected component.

System alerts

System alerts are generated for events that occur as a result of a system error. See Table 5, System Alerts, on page 37 for an explanation of system alerts.

Table 5: System Alerts

Alphanumeric Pager Code	Event	Action
20	POST timeout	**[default: Enabled]:** Generates an alert if the POST timeout value is exceeded. To configure the POST timeout value, select **System Settings** in the navigation pane, **Server Time-outs, POST watchdog**. Select a value from the drop-down menu. Click **Save** on the bottom of the screen to save the **POST Watchdog** setting.
21	O/S timeout	**[default: Enabled]:** Generates an alert if the O/S timeout value is exceeded. To configure the O/S timeout value, select **System Settings** in the navigation pane, **Server Timeouts, O/S watchdog**. Select a value from the drop-down menu. Click **Save** on the bottom of the screen to save the **O/S Watchdog** setting.
22	Test alert	Generates a manual alert if the **Generate Test Alert** button is selected.
23	Power off	**[default: Enabled]:** Generates an alert if the S8500 Media Server is turned off.
24	Power on	**[default: Enabled]:** Generates an alert if the S8500 Media Server is turned on.
25	Boot failure	**[default: Enabled]:** Generates an alert if an error occurs that prevents the S8500 Media Server from booting up.
26	Loader timeout	**[default: Enabled]:** Generates an alert if the Loader timeout value is exceeded. To configure the Loader timeout value, select **System Settings** in the navigation pane, **Server Timeouts, Loader Watchdog**. Select a value from the drop-down menu. Click **Save** on the bottom of the screen to save the **Loader Watchdog** setting.
27	PFA notification	**[default: Enabled]:** Generates an alert if a PFA notification is generated by the S8500 Media Server hardware.
	Partition configuration	Not used.

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

Monitored Local Events

The monitored local events are recorded in the event log within the RSA. These events are not sent to the administered alarm recipients.

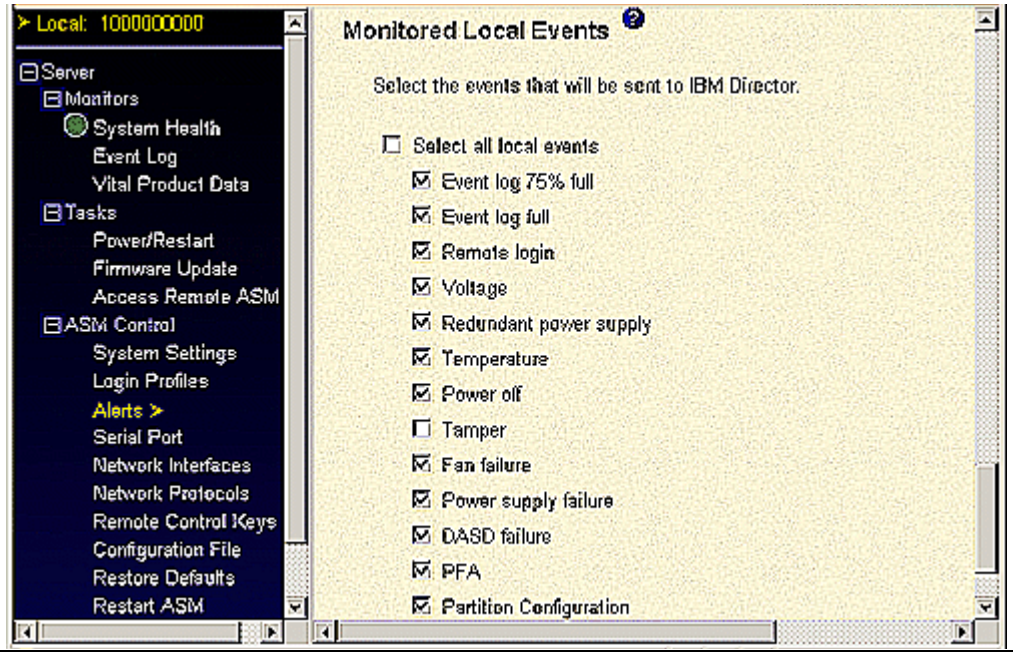
Setting local events

To set the events:

1. In the navigation pane, select **Event Log** under the **Monitors** heading.

   The Monitored Local Events window appears (see Figure 15, Monitored local events, on page 38).

Figure 15: Monitored local events



See Table 6, Monitored local events, on page 38 for an explanation of monitored local alerts.

Table 6: Monitored local events ***1 of 2***

Event	Action
Event log 75% full	**[default: Enabled]:** Generates an event if the event log reached 75% of capacity.
Event log full	**[default: Enabled]:** Generates an event if the event log reaches capacity. When the event log reaches capacity, the oldest entries in the log are deleted by new entries.
Redundant power supply failure	Not used on the S8500 Media Server configuration.
Voltage irregularity	**[default: Enabled]:** Generates an event if the monitored voltages exceed their thresholds.
Power off	**[default: Enabled]:** Generates an event if the power to the S8500 Media Server is turned off.

1 of 2

Table 6: Monitored local events ***2 of 2***

Event	Action
Power supply failure	**[default: Enabled]:** Generates an event if the power supply in the S8500 fails.
Tampering	**[default: Disabled]:** Not used in the S8500 Media Server configuration.
DASD failure	**[default: Enabled]:** Generates an event if hard disk drive failures are detected.
Remote login	**[default: Enabled]:** Generates an alert if a remote login occurs.
Temperature irregularity	**[default: Enabled]:** Generates an alert if the monitored temperatures exceed their thresholds.
Fan failure	**[default: Enabled]:** Generates an event if one of the fans fails.
PFA notification	**[default: Enabled]:** Generates an alert if any of the hardware in the S8500 generates a PFA event.
Partition configuration	Not used.
	2 of 2

2 Scroll down to the desired entry and make your changes.

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

Serial port

From the **Serial Port** window, you can:

- Configure the serial port of the RSA.
- Configure advanced modem settings.

The serial port on the RSA can be used to dial out alerts to an remote alarm recipient and provide connectivity for remote users.

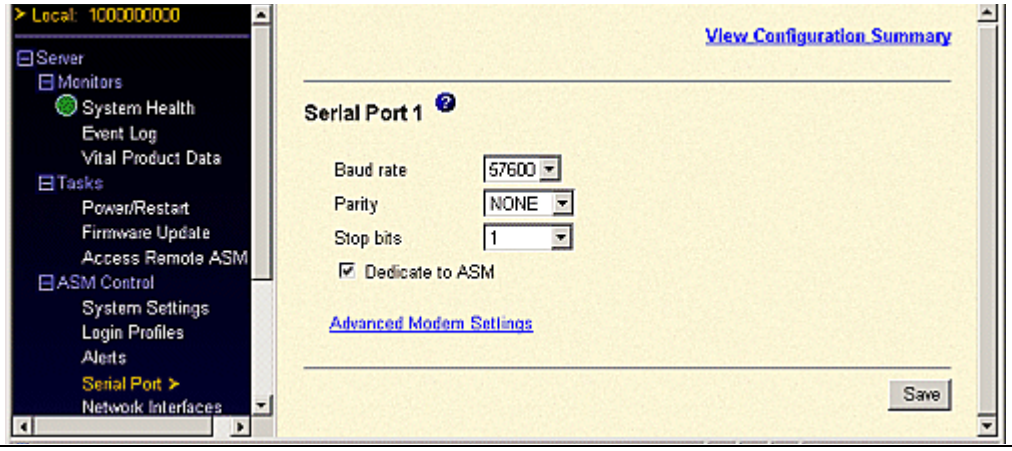
Configuring the serial port

To configure the serial port:

1 In the navigation pane, select **Serial Port** under the **ASM Control** heading.

The Serial Port window appears (see Figure 16, Serial port, on page 40).

Figure 16: Serial port



2 In the **Baud Rate [default: 57600]** field: Select the baud rate to specify the data-transfer rate of your serial port connection. Possible bits per second options that can be selected from the drop-down menu are: **2400**, **4800**, **9600**, **19200**, **38400**, and **57600**.

3 In the **Parity** field **[default: NONE]**: Select the error detection to be used for your serial port connection. Possible parity options from the drop-down menu are: **NONE**, **ODD**, **EVEN**, **MARK**, and **SPACE**.

4 In the **Stop bits** field **[default: 1]**: Select the data-terminating 1-bits or parity bit that marks the end of transmission. Possible stop bits that can be selected from the drop-down menu are: **1** and **1.5 or 2**.

NOTE:
For the following step, **Dedicate to ASM** is the only option supported by Avaya.

5 In the **Dedicate to ASM** field **[default: Enabled]**: Select the **Dedicate to ASM** check box. Failure to do so may cause the RSA not to report problems on the modem or the RSA may not answer incoming calls.

6 Click **Save,** or for advanced settings, click **Advanced Modem Settings** (see Assigning advanced modem settings on page 40).

Assigning advanced modem settings

To set the advanced modem settings:

1 After clicking **Advanced Modem Settings**, fill in the following fields:

- **Initalization string [default: ATZ^M]**: Type the initalizatiion string to be used for this specific modem.
- **Dial prefix string [default: ATDT]**: Type the initialization string to be used before the number to be dialed.
- **Hangup string [ATHO^M]**: Type the initialization string to be used to disconnect the modem.
- **Dial postfix string [default: ^M]**: Type the initialization string to tell the modem to stop dialing after the number is dialed.
- **Modem query [default: AT^M]**: Type the initialization string to be used to tell if the modem is connected.

- **Factory settings string [default: AT&FO^M]**: Type the initalization string to return the modem to factory settings.
- **Auto answer [default: ATSO=3^M]**: Type the initialization string to tell the modem to answer an incoming call after three rings.
- **Escape string [default: +++AT^M]**: Type the initialization string to return the modem to a command mode state when the modem is busy.
- **Auto answer stop [default: ATSO=O^M]**: Type the initialization string to tell the modem to stop answering the phone when it rings.
- **Caller ID string [default: no default]**: Type the initialization string that will be used to collect caller ID information from the incoming call.
- **Escape guard [default: 2.5 seconds]**: Type the length of time before and after the escape string is issued to the modem.

2 Click **Save** to save your changes.

Network interfaces

From the **Network Interfaces** window, you can:

- Set up an Ethernet connection.
- Set up a PPP over serial port connection.

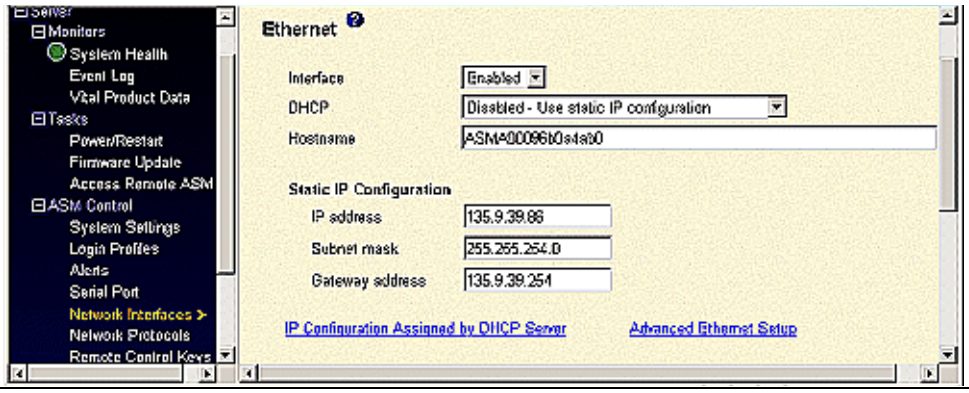
Configuring an Ethernet connection

To configure an Ethernet connection:

1 In the navigation pane, select **Network Interfaces** under the **ASM Control** heading.

The Ethernet window appears (see Figure 17, Network interfaces, on page 41).

Figure 17: Network interfaces



2. Under the **Ethernet** heading, complete the following steps:

- In the **Interface** field **[default: Enabled]**: Set to **Enabled** to use a Ethernet connection for RSA.
- In the **DHCP** field **[default: Disabled]**: Set to **Enabled** to use a Dynamic Host Configuration Protocol [DHCP).

  NOTE:
  Enabling DHCP overrides any manual settings.

- In the **Hostname** field **[default: the name of your server-RSA]**: Up to 63 characters can be entered in this field.
  - If the **DHCP** field is **Enabled** and the **Hostname** field:
    - Contains an entry, the RSA DHCP application requests that the Hostname be used by the DHCP server.
    - Is blank, the RSA DHCP application requests the DHCP server assign the Hostname to the RSA.
  - If the **DHCP** field is **Disabled**, in the **Hostname** field, type the IP hostname of the RSA.

    NOTE:
    The IP Configuration Assigned by DHCP Server link shows what the network has assigned as an address.

3. To set a static IP configuration, go to Setting a static IP configuration on page 42.

   To set an advanced Ethernet setup, go to Setting an advanced Ethernet setup on page 42.

Setting a static IP configuration

To set a static IP configuration:

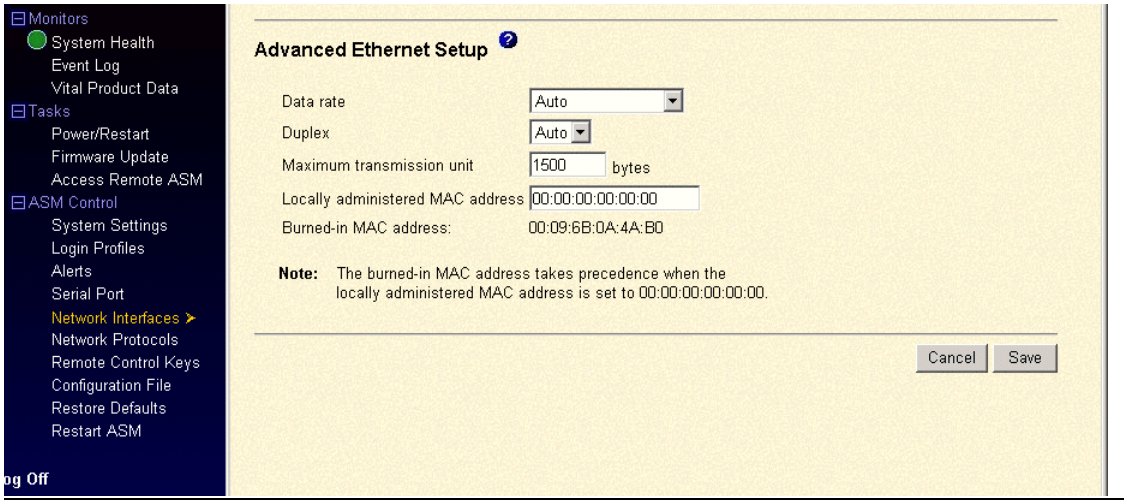
1. In the **IP address** field **[default: 192.11.13.6]**: Type the IP address only if the **DHCP** field is **Disabled**.The IP Address field should contain four intriguers from 0 through 255, separated by periods, no spaces, or consecutive periods.
2. In the **Subnet mask** field **[default: 255.255.255.254]**: Type the subnet mask only if the **DHCP** field is **Disabled.** An entry for a subnet mask field should contain four intriguers from 0 through 255, separated by periods, no spaces, or consecutive periods.
3. In the **Gateway address** field **[default: 0.0.0.0]**: Type the gateway address only if the DHCP field is **Disabled**. The gateway address should contain four intriguers from 0 through 255, separated by periods, no spaces, or consecutive periods.
4. Scroll to the bottom of the screen and click **Save**.

Setting an advanced Ethernet setup

Use the **Advanced Ethernet Setup** if you need additional Ethernet settings for data rates, transmission units, and MAC addresses.

To set an advanced Ethernet setup (see Figure 18, Advanced Ethernet setup, on page 43):

Figure 18: Advanced Ethernet setup



1. In the **Data Rate** field **[default: Auto]**: Used to specify the amount of data to be transferred per second over a LAN connection. Possible selections from the drop-down menu are: **Auto**, **10 Mb,** and **100 Mb**.
2. In the **Duplex** field **[default: Auto]**: Used to enter the type of communication channel that is used in your network. From the drop-down menu, select one of the following:
   - **Full**: Data is carried in both directions at one time.
   - **Half**: Data is carried in one direction at a time.
   - **Auto**: This option allows automatic detection of the duplex type.
3. In the **Maximum transmission unit** field **[default: 1500 bytes]**: Used to specify the maximum packet size, in bytes, for your network interface.
4. In the **Locally administered MAC address** field **`[0.0.0.0]`**: A locally administered MAC overrides the burned-in MAC address. The locally administered MAC address must be in the following format:
   - Hexadecimal value from 000000000000 through FFFFFFFFFFFF.
   - In the form of XX:XX:XX:XX:XX:XX where X is a number between zero and nine.
5. In the **Burned-in MAC address** field: This is a read-only field that contains the unique factory MAC address burned-in at the factory.

   NOTE:
   The RSA does not support the use of a multicast address. When a multicast address is used the least significant bit of the first byte is set to one.

6. Click **Save** to save the changes.
7. In the navigation panel, click **Restart ASM** under the **ASM Control** heading to activate the changes.

Configuring PPP access over a serial port

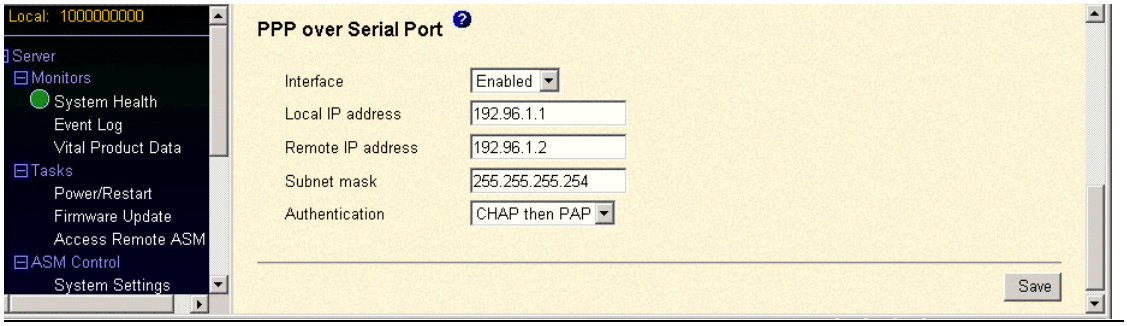
Use the point-to-point (PPP) access method if you do not have Ethernet access.

> **NOTE:**
> Use PPP over the serial port for remote access to the RSA.

To configure PPP over the serial port:

1. In the navigation pane, select **Network Interfaces** under the **ASM Control** heading.
2. Scroll down to the **PPP over Serial Port** selection (see Figure 19, PPP over Serial Port, on page 44).

Figure 19: PPP over Serial Port



3. In the **Interface** field **[default: Disabled]**: Select **Enabled** to use PPP over the serial port.
4. In the **Local IP address** field **[default: 10.4.0.1]**: Type the local IP address for the PPP interface on the RSA. The IP address must consist of four integers ranging from 0 to 255, separated by periods, no spaces or consecutive periods.
5. In the **Remote IP address** field **[default: 10.4.0.2]**: Type the remote IP address that the RSA assigns to a remote user. The remote IP address must consist of four integers ranging from 0 to 255, separated by periods, no spaces or consecutive periods.
6. In the **Subnet mask** field **[default: 255.255.255.254]**: Type the subnet mask for the RSA. The subnet mask must consist of four integers ranging from 0 to 255, separated by periods, no spaces or consecutive periods.
7. In the **Authentication** field **[default: CHAP then PAP]**: Select the type of authentication protocol that will be negotiated for a PPP connection:
   - **CHAP then PAP**: When using this setting, authentication tries using CHAP first. If CHAP was unsuccessful, then PAP is tried as a secondary protocol.
   - **PAP Only**: When using this setting, a two-way handshake procedure is used to validate the identity of the incoming caller. PAP must be used if a plain text password must be available to simulate a login at a remote host.
   - **CHAP Only**: When using this setting, a three-way handshake procedure is used to validate the identity of the incoming caller and any time after the call is established. CHAP protects against playback and trial-and-error attacks.
8. Click **Save** to store the changes.
9. You must restart the ASM to activate the **Network Protocols** changes. To restart ASM, select **Restart ASM** under the **ASM Control** heading in the navigation pane.

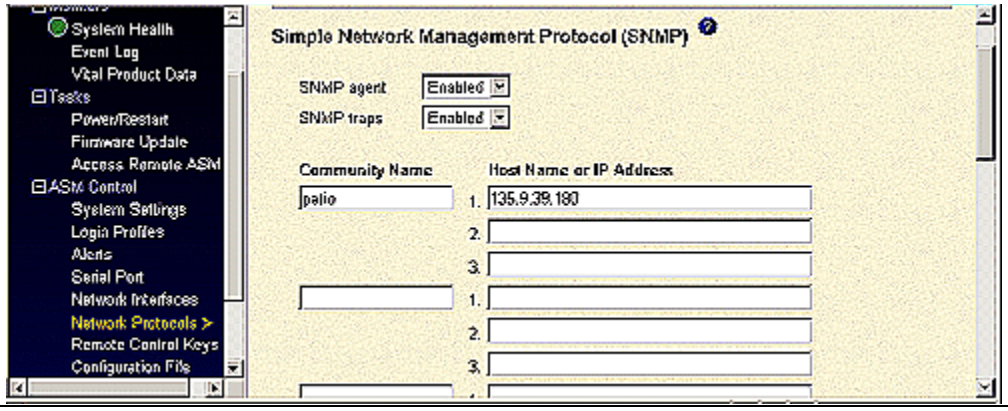
Network protocols

From the **Network Protocols** window, you can configure the:

- Simple Network Management Protocol [SNMP] setup.
- Domain Name System [DNS] setup.
- Simple Mail Transfer Protocol [SMTP] setup.

See Figure 20, Network protocols, on page 45 for the Simple Network Management Protocol (SNMP) window.

Figure 20: Network protocols



Enabling SNMP agents and traps

Use the **SNMP** window under Network Protocols to enable SNMP agents and traps, and to establish community names with their related host name or IP address.

To enable SNMP agents and traps:

1. In the navigation pane, select **Network Protocols** under the **ASM Control** heading.
1. In the **SNMP agent** field **[default: Disabled]**: Use this field to enable or disable the SNMP agent.
2. In the **SNMP traps** field **[default: Enabled]**: Use this field to enable or disable the SNMP traps.

   NOTE:
   The following criteria must be met before enabling SNMP agent and traps:

   - Both the **SNMP agent** and the **SNMP trap** fields must be **Enabled** before an SNMP alert can be sent.
   - The **Contact** and **Location** fields must be filled out in the ASM Information section of the System Settings window. For more information on the ASM Information fields, see System settings.
   - At least one SNMP community with valid IP address or host name must be configured.

3. **Community Name [no default]**: Use this field to type a name or authentication string that defines the community that will receive the SNMP alerts.

4. **Host Name or IP Address [no default]**: In the field that corresponds with the Community Name, type the IP Address or Host Name for each community manager.
5. If a DNS server is not used or available, scroll down and click **Save**. If a DNS server will be used, continue to Enabling DNS on page 46 before restarting the ASM.

   NOTE:
   You must restart the ASM to activate the Network Protocols changes.

6. To restart the ASM, click **Restart ASM** under the **ASM Control** heading in the navagation pane.

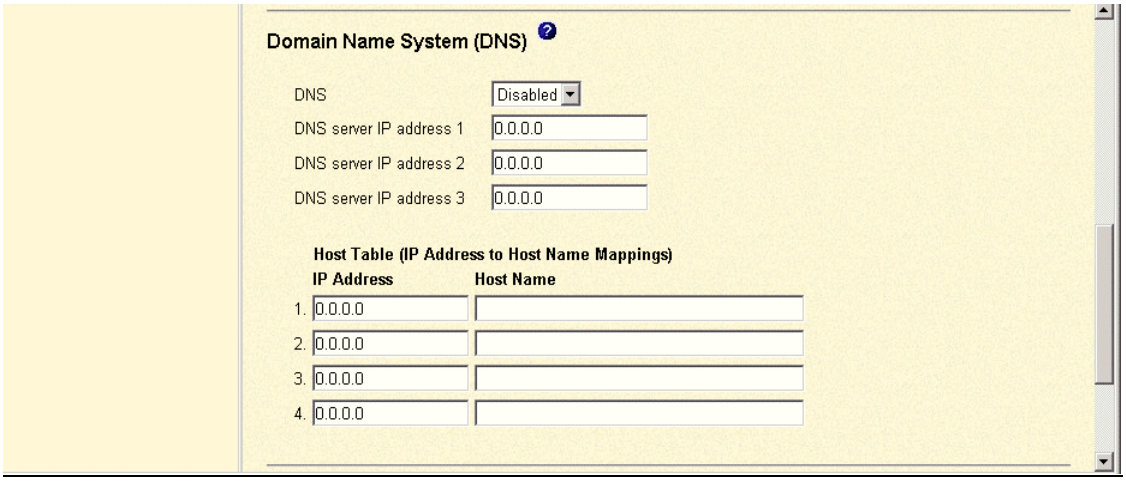
Enabling DNS

To enable the Domain Name System (DNS) and specify the DNS IP address:

1. In the navigation pane, select **Network Protocols** under the **ASM Control** heading.

   The Simple Network Management Protocol (SNMP) window appears.
2. Scroll down to the DNS section (see Figure 18, Advanced Ethernet setup, on page 43).

Figure 21: DNS



3. In the **DNS** field **[default: Disabled]**: Select **Enabled** from the drop-down menu if a DNS server will be used.
4. In the **DNS server IP address 1, 2, and 3** fields **[default: 0.0.0.0]**: You can specify up to three DNS server IP addresses once the **DNS** field is **Enabled**. Each IP address should contain integers 0 through 255, separated by periods.
5. Scroll to the bottom of the page and click **Save**.

   NOTE:
   You must restart the ASM to activate the Network Protocols changes.

6. To restart the ASM, select **Restart ASM** under the **ASM Control** heading in the navigation pane.

SMTP

This section must be completed if a SMTP server is being used.

1. In the navigation pane, select **Network Protocols** under the **ASM Control** heading.
2. **SMTP Server Host Name or IP Address** field **[no default]**: If a DNS server is being used, type the hostname of the SMTP Server. If a DNS server is not being used, type the IP Address associated with the SMTP server.
3. Scroll to the bottom of the page and click **Save**.

Accessing the configuration window

Use the Configuration window to:

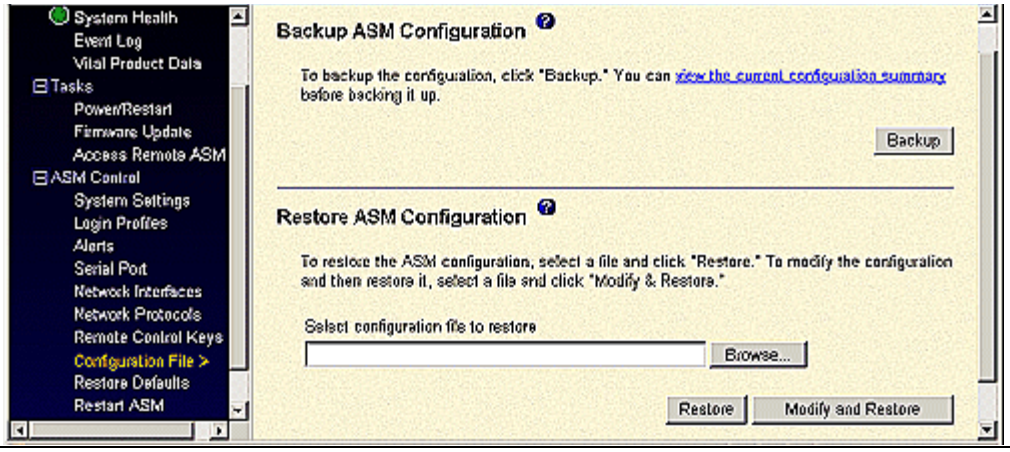
- Back up the ASM configuration
- Restore and Modifying the ASM configuration

To access the Configuration window:

1. In the navigation pane, select **Configuration File** under the **ASM Control** heading.

   The Configuration window appears (see Figure 22, Configuration file, on page 47).

Figure 22: Configuration file



A copy of the ASM backup is stored on the S8500 Media Server. You can use this backup copy to restore the RSA configuration in the event of damage or corruption. You also can modify the saved configuration file before restoring it on the RSA.

Backing up the ASM configuration

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

To backup the ASM configuration:

1. Log in to the RSA. Refer to Connecting and logging in to the RSA for more information.
2. In the navigation pane, select **Configuration File** under the **ASM Control** heading.
3. In the **Backup ASM Configuration** section, select **view the current configuration summary**.
4. Verify that these are the settings that you want to save, then click **Close**.
5. In the **Backup ASM Configuration** section, click **Backup**.
6. Type a name for the backup and choose a location where the backup files will be stored.
7. Click on:
   - For Windows Internet Explorer: Select **Save this file to disk**, and then **OK**.
   - For Netscape Navigator: Select **Save File**.

Restoring and modifying the ASM configuration

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

To restore or modify the saved configuration file:

1. Log in to the RSA. Refer to Connecting and logging in to the RSA for more information.
2. In the navigation pane, select **Configuration File** under the **ASM Control** heading.
3. In the **Restore ASM Configuration** section, click **Browse**.
4. Find and click on the configuration file. Click **Open**.

   The file, including the full path name, appears in the box.
5. To modify the file before restoring, go to Step 6. To restore the file without modifying it, go to Step 7.
6. To modify the file before restoring:
   - Click **Modify and Restore**. A new window opens showing only the fields that can be modified.
   - Click the text box corresponding to the field you wish to change. Type the new data.
   - To toggle between the view that you are modifying and the complete configuration view, then click **Toggle View**.
   - Once the changes to the configuration file have been made, click **Restore Configuration** to restore the modified file.
   - Continue with step 8.
7. To restore a file without modifying, click **Restore**.
8. After selecting **Restore** or **Restore Configuration**, a progress indicator appears.

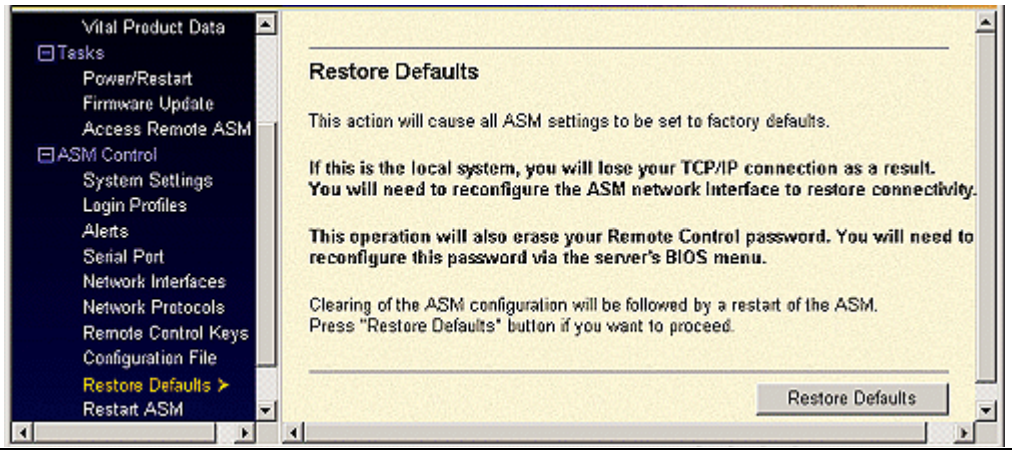
   A confirmation window opens when the update is completed successfully.
9. Click **Restart ASM** under the **ASM Control** heading and then click **Restart**.
10. Click **OK** to confirm that you would like to restart the RSA.
11. Click **OK** to close your current browser window.

Restoring ASM defaults

NOTE:
You must have read/write privileges on your login ID to use this option.

You can use the Restore ASM section to restore the RSA to factory settings. See Figure 23, Restore defaults, on page 49.

Figure 23: Restore defaults



WARNING:
Executing the **Restore ASM Defaults** option removes the Avaya defaults. Avaya defaults can be restored manually using the information found in the Avaya RSA Defaults section or by restoring the Avaya default file. The Avaya default file can be found at http://support.avaya.com or on the Communication Manager 2.0 CD for Linux Servers and Gateways. For instructions on restoring the default file, see Restoring and modifying the ASM configuration.

WARNING:
Executing the Restore ASM Defaults option removes all the modifications made to the RSA.

To restore ASM defaults:

1. Log into the RSA. For more information on how to log into the RSA, see Connecting and logging in to the RSA on page 20.

   CAUTION:
   You will loose your Ethernet connection. All modifications and Avaya defaults are removed and you will not be able to log into the RSA.

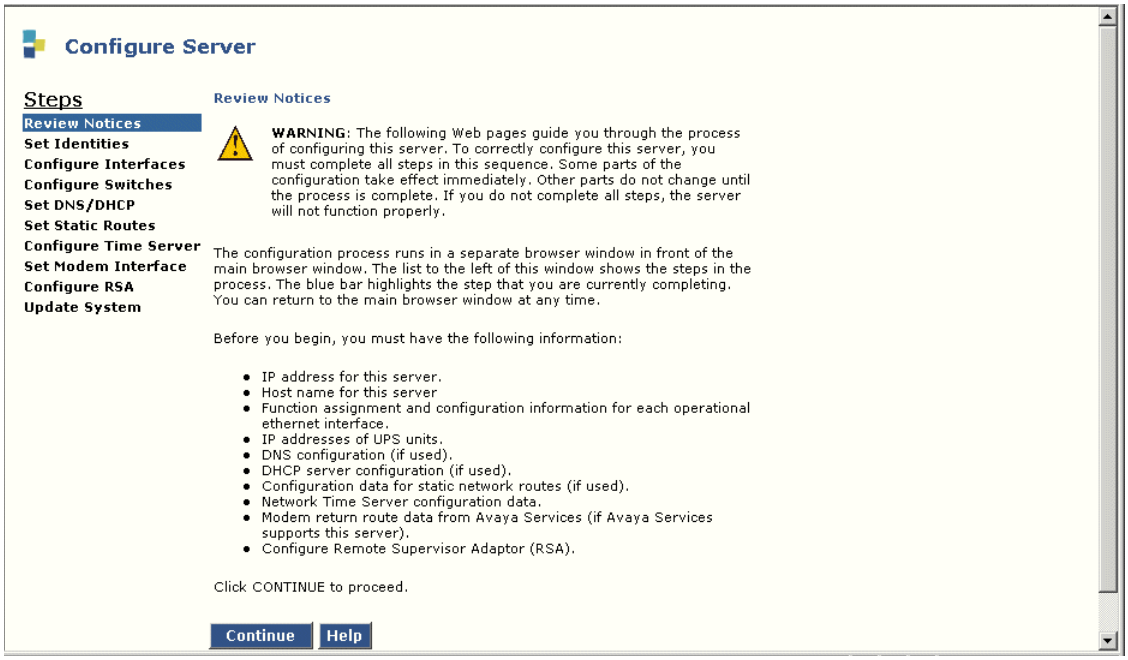
2. In the navigation pane, select **Restore Defaults** under the **ASM Control** heading.
3. Click **Restore Defaults**.

Restoring the Avaya defaults

If you have ignored the warnings in Restoring ASM defaults or you need to reset the RSA card to Avaya defaults:

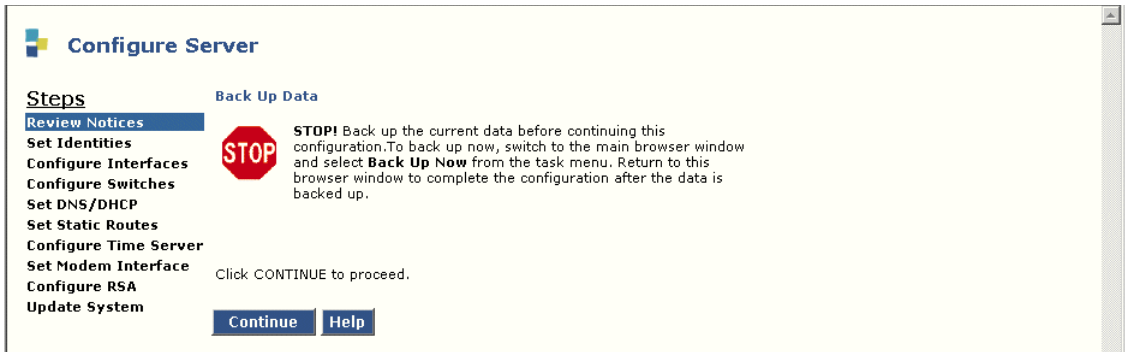
1. On a Web browser, in the **Address** field, type http://support.avaya.com and download the configuration file.
2. On a Web browser, select **Launch Maintenance Web Interface** on the server.
3. Under the **Server Configurations** heading, select **Configure Server**.

   The Review Notices window appears.



4. Click **Continue**.

   The Back Up Data window appears.

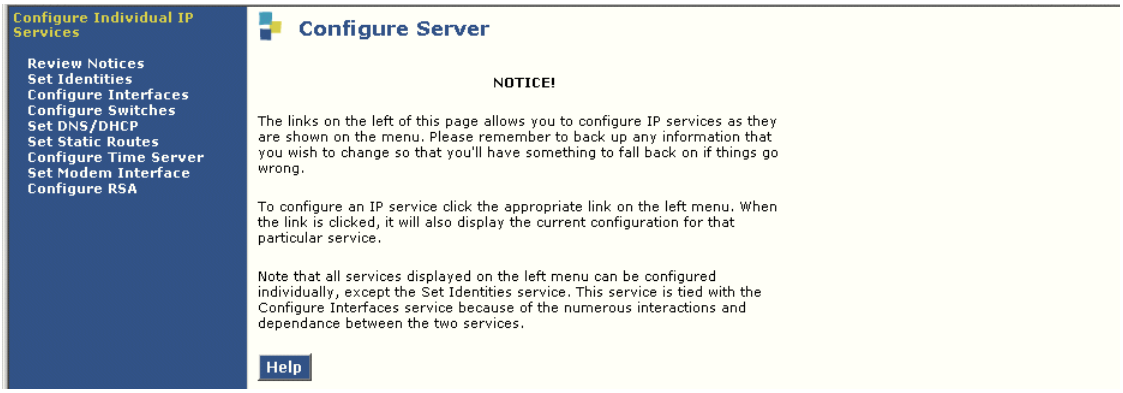


5 Click **Continue**.

The Specify how you want to use this wizard window appears.

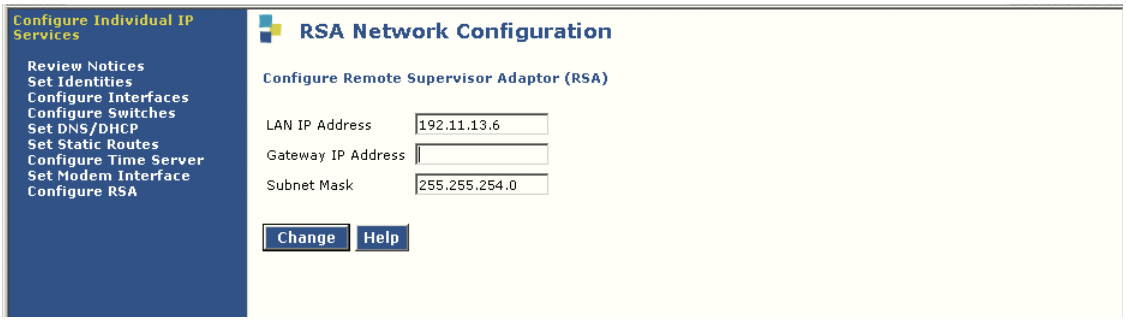
6 Select **Continue individual services** and click **Continue**.

The Notice window appears.



7 In the left menu, click **Configure RSA**.

The Configure Remote Supervisor Adapter (RSA) window appears.



8 In the **LAN IP Address** field, type **192.11.13.6**.

9 In the **Subnet Mask** field, type **255.255.254.0** and click **Change**.

10 Plug the cross-over cable into the RSA card.

11 Proceed to Restoring and modifying the ASM configuration on page 48 and use the file you downloaded in step 1.

Restarting the RSA

Use the **Restart ASM** option to restart the RSA. While configuring the RSA, you will be prompted to use this option to make changes permanent.

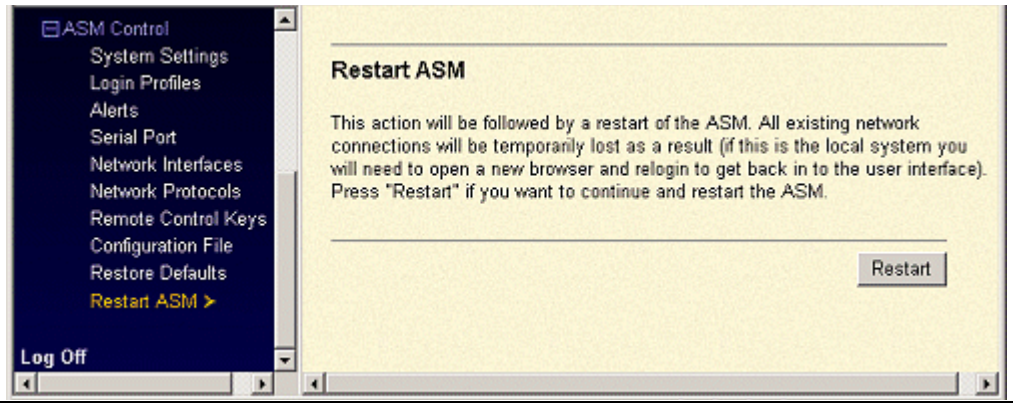
To restart the RSA:

> **NOTE:**
> You must have read/write privileges on your login ID to use this option.

1. Log into the RSA. For more information on how to log into the RSA see Connecting and logging in to the RSA on page 20.
2. In the navigation pane, select **Restart ASM** under the **ASM Control** heading.

   The Restart ASM window appears (see Figure 24, Restart ASM, on page 52).

Figure 24: Restart ASM



> **NOTE:**
> You will loose your Ethernet connection. Once the restart is completed, open a new browser and log back into the RSA.

3. Click **Restart**.

Logging off the RSA

Use this option to log off:

- The RSA.
- ASM processor.
- Another remote server.

To log off the RSA:

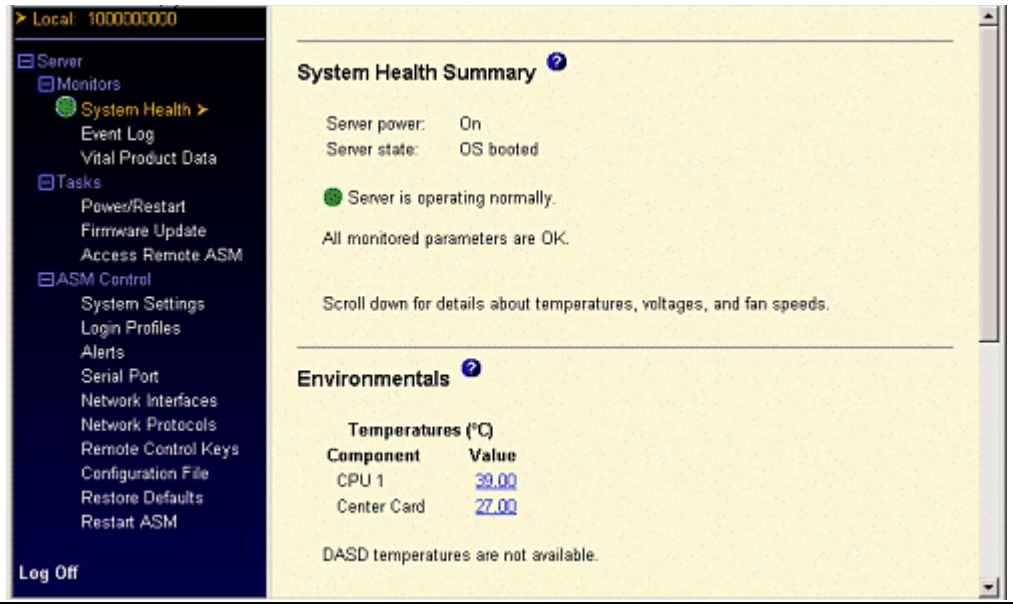
1. In the navigation pane, select **Log Off**.
2. In the confirmation window, click **Yes**.

Monitoring the S8500 using the RSA

The following information can be found under the **Monitors** heading (see Figure 25, System health, on page 53):

- System Health:
  - Monitors the temperature, voltage, and power readings of the S8500 Media Server
  - View the fan health
  - View the status of the operating system
- Event Logs:
  - View the events recorded in the logs
  - View the severity of the events
- VPD: This feature is not supported as part of the S8500 Media Server Configuration.

Figure 25: System health



Viewing system health summary

To view the System Health of the S8500 Media Server, select **System Health** under the **Monitors** heading in the navigation pane. The following information appears under the **System Health Summary**:

- Server power: Indicates the server is either On or Off.
- Server state: Shows the current state of the S8500 Media Server.

A circle that indicates the overall health of the S8500 Media Server:

- Green: Indicates that the S8500 Media Server is operating normally
- Red circle with an X: One or more monitored parameters are abnormal.
- Yellow triangle with an exclamation point: One of more monitored parameters are abnormal.

If the circle is either red or yellow: more detailed information concerning the problem can be found in the System Health Summary section.

Environmentals

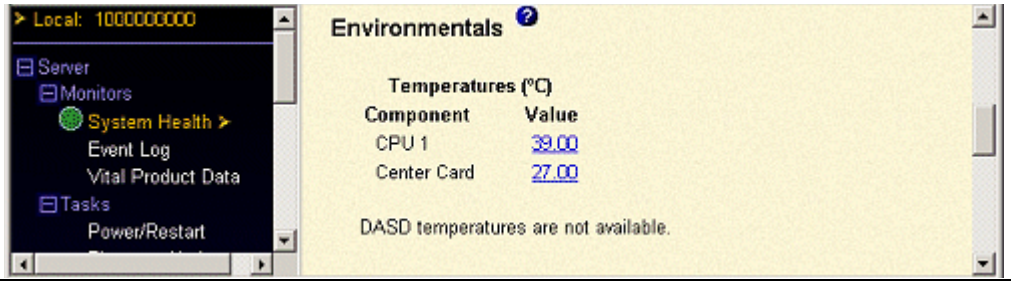
The RSA monitors current temperature readings and threshold levels for various components of the S8500 Media Server. To obtain more information about a specific value, click on the number associated with the component under the **Value** field.

Temperature thresholds

The RSA tracks the current temperature readings and threshold levels for system components.

The temperatures section displays the values the RSA reacts to when reached or exceeded (see Figure 26, System health temperatures, on page 54). The values are not programable and cannot be changed.

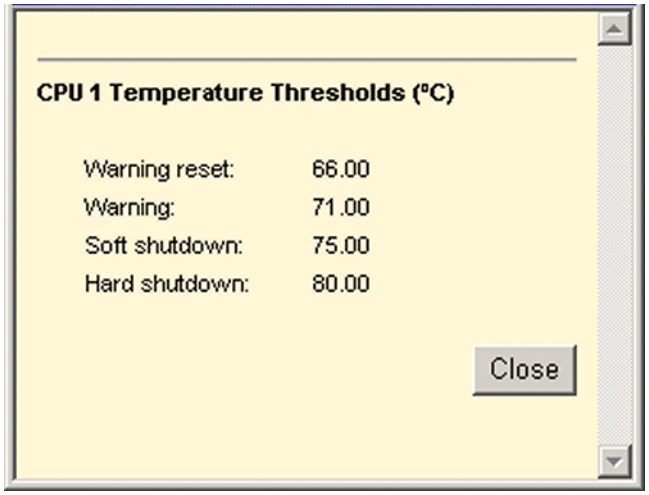
Figure 26: System health temperatures



NOTE:
You must check the temperature box under the **Alerts** section for a temperature alert to be sent to the configured alert recipients.

When you click on a specific value associated with a component, a window similar to Figure 27, System health temperature thresholds, on page 55 opens.

Figure 27: System health temperature thresholds



The reported temperatures for system components are measured in the following ranges:

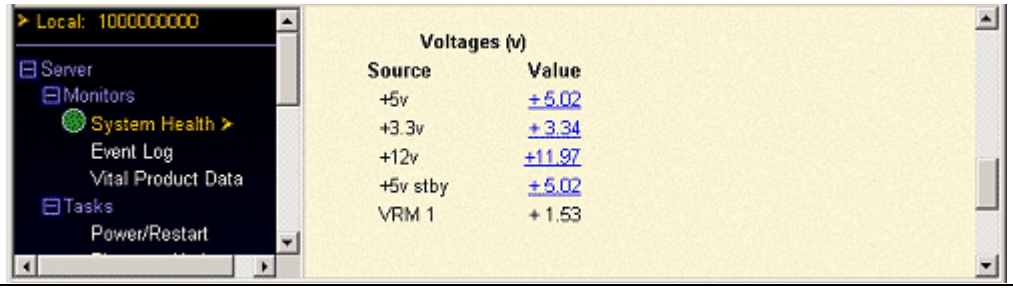
- **Warning Reset**: If the temperature returns to a value below the warning reset value, the RSA assumes that the temperature has returned to normal and does not generate any further alerts.
- **Warning**: If the temperature reaches or exceeds the value specified for a warning, an alert is generated.
- **Soft Shutdown**: When the temperature reaches or exceeds the value specified for a soft shutdown, a second temperature alert is sent and the RSA begins the shutdown of the S8500 Media Server. The shutdown will be an orderly operating-system shutdown. The S8500 Media Server turns itself off when the shutdown completes.
- **Hard Shutdown**: When the temperature reaches or exceeds the value specified for a hard shutdown, the S8500 Media Server immediately shuts down. The RSA sends out an alarm to the configured alert recipients.

Voltage thresholds

The RSA sends an alert if any monitored power source voltage falls outside the specified operational ranges.

The voltages section displays the values RSA reacts to when reached or exceeded (see Figure 28, System health voltage, on page 55). The values are not programable and cannot be changed.

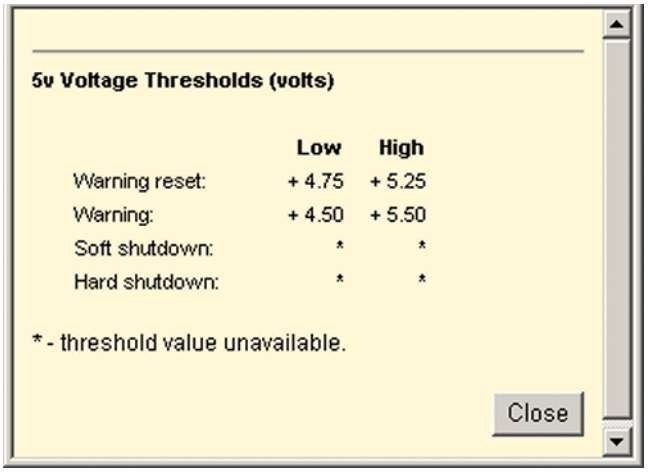
Figure 28: System health voltage



NOTE:
You must check the **Voltage** box under the **Alerts** section for a voltage alert to be sent to the configured alert recipients.

When you click on a specific value associated with a component, the following window opens.

Figure 29: System health voltage thresholds



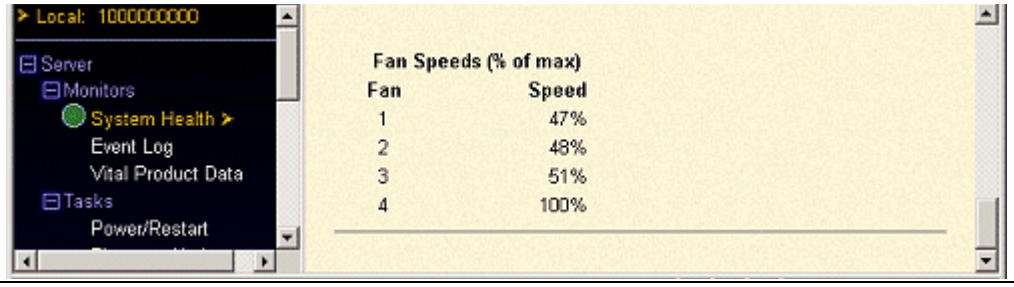
The reported voltages for the designated system components are measured in the following ranges:

- **Warning Reset**: If the voltage returns to a value below the warning reset value, the RSA assumes that the voltage has returned to normal and does not generate any further alerts.
- **Warning**: If the voltage reaches or exceeds the value specified for a warning, an alert is generated.
- **Soft Shutdown**: When the voltage reaches or exceeds the value specified for a soft shutdown a second voltage alert is sent and the RSA begins the shutdown of the S8500 Media Server. The shutdown will be an orderly O/S shutdown. The S8500 Media Server turns itself off when the shutdown completes.
- **Hard Shutdown**: When the voltage reaches or exceeds the value specified for a hard shutdown, the S8500 Media Server immediately shuts down. The RSA sends out an alarm to the configured alert recipients.

Fan speed

The RSA monitors the fan running speed of the S8500 Media Server (see Figure 30, System health fan speed, on page 57). The speed is express in a percentage of the maximum fan speed. A fan alert is generated if the fan speed drops in an unacceptable level or the fan stops.

Figure 30: System health fan speed



NOTE:
You must check the associated fan box under the **Alerts** section for that fan alert to be sent to the configured alert recipients.

The event log

The Event Log page contains all entries that currently are stored in the server event log and POST event log. Information concerning all remote access attempts and dial-out events is recorded in the RSA or ASM processor event log.

Viewing the event log

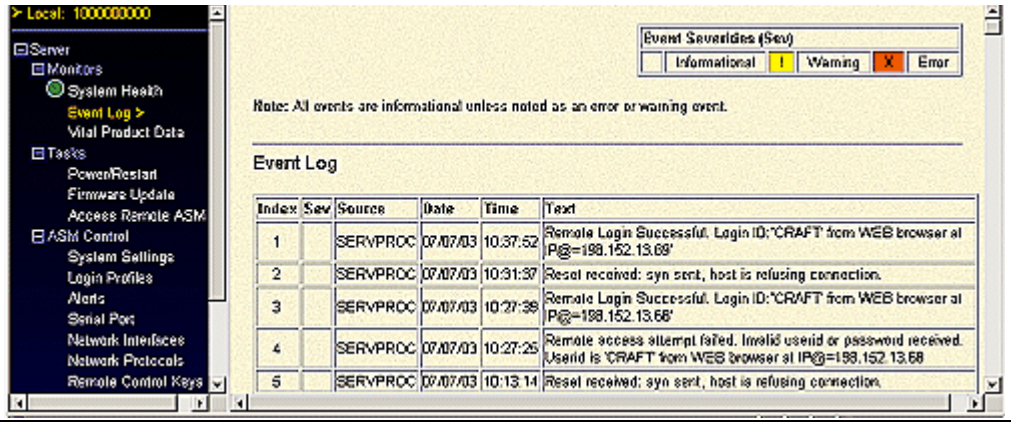
The Remote Supervisor Adapter and ASM processor time stamps all events and logs them into the event log. Information such as, all login attempts, dial-out attempts, memory errors, and bus failures are all contained within the event log. Color indicators highlight the informational, warning, and error entries

To view the event log:

1. In the navigation pane, select **Event Log** under the **Monitors** heading.

   The Event Log window appears (see Figure 31, Event log, on page 57).

Figure 31: Event log



2. Scroll down to view the complete contents of the event log.

The event log consists of the following fields:

- **Index**: The assigned number that can be used to identify the entry.
- **Sev**: Three possible severities can be assigned to any given entry in the log:
  - **Informational**: This low severity is assigned to entries in which you should take note.
  - **Warning**: This severity level is assigned to any entry that could affect the performance of the S8500 Media Server.
  - **Error**: This severity level is assigned to any entry that needs immediate attention.
- **Source**: The entity logging the event.
- **Date**: The date of the entry into the event log.
- **Time**: The time of the entry into the event log.
- **Text**: A description of the nature of the event.

Clearing the event log

Size for the event log is limited. When the limit for the event log is exceeded, older entries are deleted in a first-in, first-out order.

To clear the event log:

1. Scroll to the bottom of the Event Log window.
2. Click **Clear Log**.

Saving the event log

To save the current event log to a file:

1. Scroll to the bottom of the Event Log window and click **Save Log as Text File**.
2. A file download window opens that identifies the filename and the originating source. Click **Save** in the file download window to proceed with the file download.
3. A **Save As** window opens. Select the location on your computer that you want the file to be saved in and click **OK**.
4. A **Download Complete** window opens when the file has been copied to the location specified on the disk. You can use MicroSoft Excel to open the file for viewing.

Vital product data

Upon S8500 Media Server startup, the RSA collects system, basic input/output (BIOS) information, and server component vital product data (VPD) and stores it in non-volatile memory. The VPD page contains key information about the remote managed server that the RSA is monitoring.

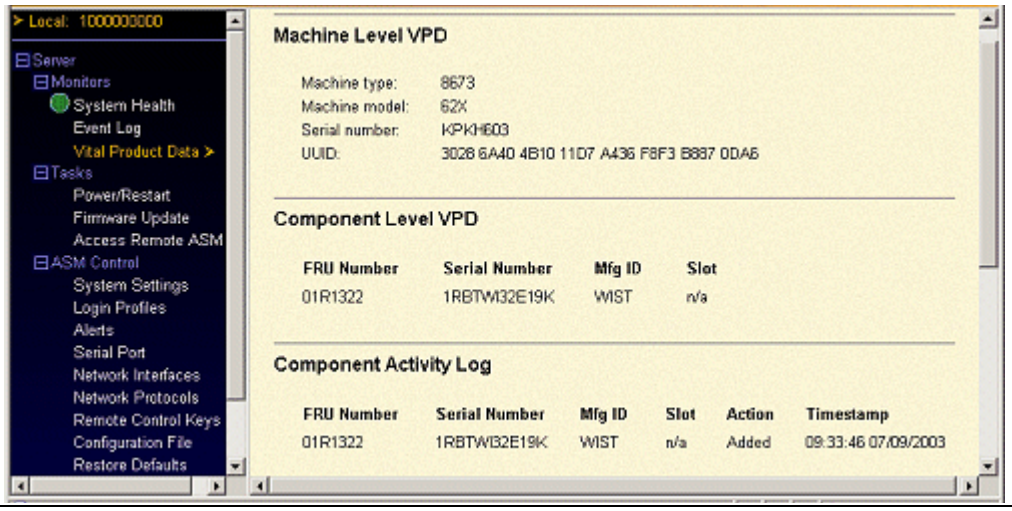
Viewing vital product data

To view the VPD data for the S8500 Media Server:

1. Log into the RSA. For information, see Connecting and logging in to the RSA on page 20.
2. In the navagation pane, select **Vital Product Data** under the **Monitors** heading.

   The VPD window appears (see Figure 32, Vital product data, on page 59).

Figure 32: Vital product data



3. Scroll down to view the VPD readings listed in the following tables.

Table 7: Machine level VPD

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

Component level VPD

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

Table 8: Component level VPD data

Field	Function
Firmware Type	Identifies the ASM firmware component type: main application, boot ROM, or remote control.
FRU Number	Identifies the field replaceable unit (FRU) number (a seven-digit alphanumeric identifier) of each component.
Serial Number	Identifies the serial number of each component.
Mfg ID	Identifies the manufacturer ID for each component.
Slot	Identifies the slot number where the component is located.

Component activity log

You can find a record of component activity as listed in the following tables.

Table 9: Component activity log

Field	Function
FRU Number	Identifies the field replaceable unit (FRU) number (a seven-digit alphanumeric identifier) of the component.
Serial Number	Identifies the serial number of the component.
Mfg ID	Identifies the manufacturer ID for 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 each component action. The date displays in the MM/DD/YY format. The time displays in the HH:MM:SS format.

POST/BIOS VPD

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

Table 10: POST/BIOS VPD

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

ASM VPD

You can find vital product data for the RSA in this section.

Table 11: ASM vital product data

Field	Function
Firmware Type	Identifies the ASM firmware component type: main application, boot ROM, or remote control.
Build ID	Identifies the build IDs of the application firmware and the startup ROM firmware.
File Name	Identifies the file names of the application firmware and the startup ROM firmware.
Released	Identifies the release dates of the application firmware and the startup ROM firmware.
Revision	Identifies the revision numbers of the application firmware and the startup ROM firmware.

Performing RSA tasks

The **Tasks** section allows you to view the S8500 Media Server power and restart activity, and to directly control the S8500 Media Server. Using the **Server Power / Restart Control** option, you can perform the following functions:

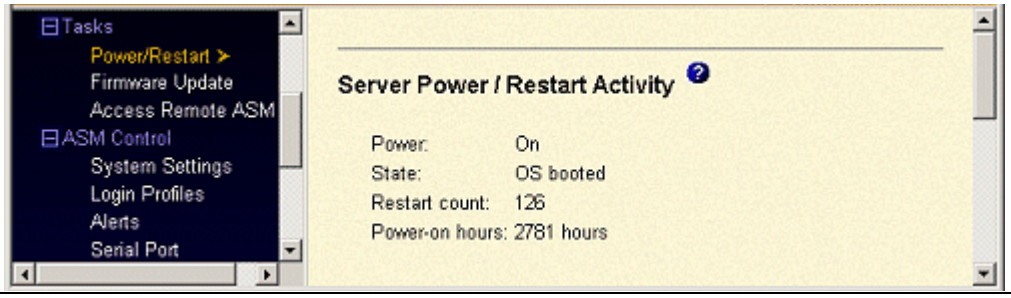
- Power on server immediately
- Power on server at a specified time
- Power off server immediately
- Shutdown O/S and then power off server
- Shutdown O/S and then power restart server
- Restart the server immediately

NOTE:
You must have read/write permissions to perform the functions under the **Tasks** heading.

Server power and restart activity

The Server Power and Restart Activity section displays the power state of the S8500 Media Server at the time the Web screen was generated. See Figure 33, Server power/restart activity, on page 62.

Figure 33: Server power/restart activity



Field entries within this section include:

- **Power**: System power on, system power off, or state unknown
- **State**: This field shows the state of the S8500 Media Server at the time the 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
  - In OS
  - CPUs held in reset
  - System power on/before POST

  NOTE:
  The restart counter is set to 0 (zero) if the RSA is defaulted to factory settings.

- **Restart Count**: This field shows the number of times the S8500 Media Server has been restarted.
- **Power-on Hours**: This field shows the number of hours the S8500 Media Server has been powered on.

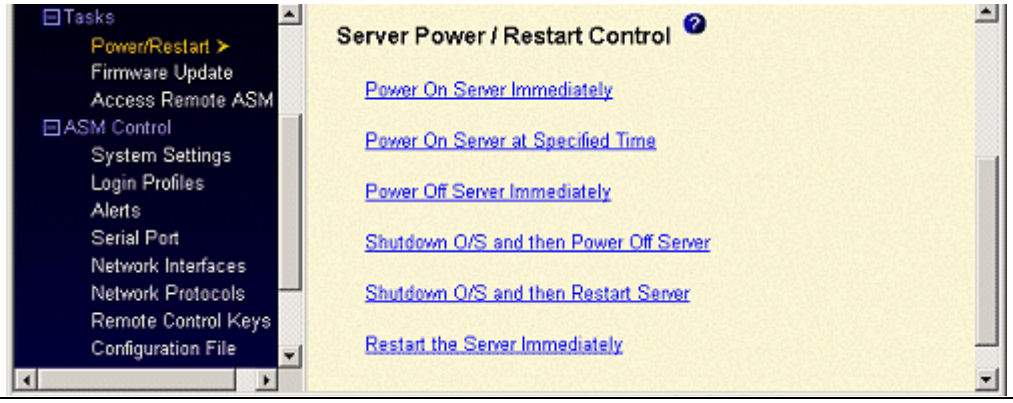
Accessing server power and restart control

You can power-on, power-off, and restart the S8500 Media Server using the **Server Power / Restart Control** option on the RSA Web interface.

To access the **Server Power / Restart Control** option:

1 In the navigation pane, select **Power/Restart** under the **Tasks** heading. The Server Power/Restart Control window appears (see Figure 34, Server power/restart control, on page 63).

Figure 34: Server power/restart control



2 Scroll down to the Server Power / Restart Control section.

3 Select one of the following options:

- **Power on Server Immediately**: Click on this link to immediately power on the S8500 Media Server.
- **Power on Server at Specified Time**: Click on this link to power the S8500 Media Server down at a specific time. A new window opens that displays the current date and time. Enter the following data:
  - **Time of day to power on the server**: Type the time of day that you wish to power-on the S8500 Media Server. Time of day must be in a 24 hour format (hh:mm).
  - **Date to power on server**: Type the date that you wish to power-on the S8500 Media Server.

CAUTION:
The following option does not shut down the O/S before the S8500 is powered off.

- **Power off Server Immediately**: Click on this link to immediately power off the S8500 Media Server.
- **Shutdown O/S and then Power Off Server**: Click on this link to shut down the operating system and then power off the S8500 Media Server.
- **Shutdown O/S and then Restart Server**: Click on this link to reboot the operating system and restart the S8500 Media Server.

CAUTION:
The following option does not shut down the O/S before restarting the S8500 Media Server.

- **Restart the Server Immediately**: Click on this link to reboot the S8500 Media Server.

NOTE:
A confirmation window appears when you choose to power on, power off, or restart the S8500 Media Server.

Updating RSA or BIOS firmware

This option updates the firmware of the RSA or the server (BIOS) in which it is installed. Updating the firmware also enables the BIOS code, diagnostics, power backplane, front panel, and the serial peripheral interface (SPI) of the server in which the RSA is installed.

If available, new RSA and BIOS firmware can be downloaded from http://support.avaya.com.

To update the RSA firmware:

1. Click on the file.

   A download window opens.

2. Select the name and location for the file you are downloading and click **OK**.

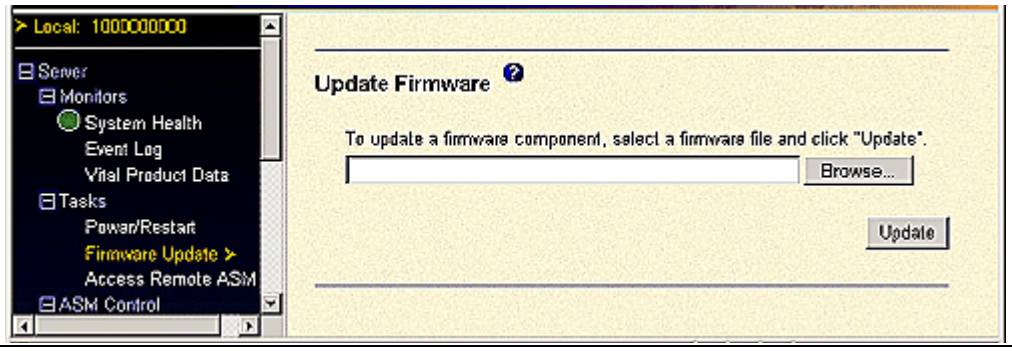
   A progress window opens as the files are transferred to the selected location. A confirmation window opens when the transfer is completed.

3. Log in to the RSA. See Connecting and logging in to the RSA for log in instructions.

4. In the navigation pane, select **Firmware Update** under the **Tasks** heading.

   The Update Firmware window appears (see Figure 35, Update firmware, on page 64).

Figure 35: Update firmware



5. Click **Browse**. Go to the saved location from step 3.

6. Click **Open** to select the cnetbrus.pkt file and have it appear in the box beside **Browse**.

7. Click **Update** to begin the firmware update. A progress window opens as the files are transferred to temporary storage on the RSA.

   A confirmation window opens when the transfer is complete.

8. Verify that the file in the confirmation window is the file that you wish to use for the update. If you do not wish to continue with the update, click **Cancel**.

9. To continue with the firmware update, click **Continue**.

   A progress window opens as the firmware on the RSA updates. A confirmation window appears when the update is completed.

10. Repeat Step 4 through Step 9 each time to update the cnetmnus.pkt and cnetrgus.pkt files.

NOTE:
You should update all three components (cnetbrus.pkt, cnetmnus.pkt and cnetrgus.pkt) from the Avaya support website before restarting the RSA.

11. After you receive the confirmation window, click **Restart** to restart the RSA.
12. Click **OK** to continue with the restart.
13. Click **OK** to close the browser window.
14. Log in to the RSA. See Connecting and logging in to the RSA for log in instructions.

Accessing remote ASM

This feature is not supported as part of the S8500 Media Server Configuration.

Glossary

A

ASM
Advanced System Management on the RSA provides an interface to view the health of monitored components and configuration settings, and administer the settings for the RSA.

ART
Avaya Registration Tool is a web-based program that permits Avaya employees to perform product registrations and related procedures automatically.

B

BIOS
Basic Input/Output System. A built-in software that knows what a computer can do without accessing any programs from the disk. The BIOS contains all the code required to control the keyboard, display screen, disk drives, and a number of miscellaneous functions.

D

DAST
Direct Access Storage Device. Another name for a disk drive.

L

Loader
An operating system utility that copies programs from a storage device to main memory where it can be executed. In addition, the loader can replace a virtual address with a physical address.

O

Operating System
A software platform on which other programs, called software applications, can run. Also performs key computer functions such as keyboard input and screen display. The O/S for the S8500 is Linux Red Heat.

P

PFA
Predictive Failure Analysis monitors the hard disk for key device performance indicators that change over time or exceed specified limits. A PFA notification generates an alert.

POST
Power On Self Test. A diagnostic testing sequence that is run by a computer's BIOS when the power is initially turned on. The POST determines if the RAM, disk drives, and other hardware components are working properly.

Index

I

L

M

N

O

P

R

S

T

V

W