Converged Communications Server R3.0

Installation and Administration Guide

(SIP Enablement Services R3.0)

555-245-705
Issue 5.1
July 2005

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.

Disclaimer

Avaya is not responsible for any modifications, additions or deletions to the original published version of this documentation unless such modifications, additions or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

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 Contacts* link that is located under the *Support Tools* heading. Then click the appropriate link for the type of support that you need.
- Outside the United States, click the *Escalation Contacts* link that is located under the *Support Tools* heading. 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, or IEC 60950-1, 1st 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, or CAN/CSA-C22.2 No. 60950-1-03 / UL 60950-1.

Safety Requirements for Information Technology Equipment, AS/NZS 60950:2000.

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 used in Avaya equipment typically operate within the following parameters:

Typical Center Wavelength	Maximum Output Power
830 nm - 860 nm	-1.5 dBm
1270 nm - 1360 nm	-3.0 dBm
1540 nm - 1570 nm	5.0 dBm

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, EN55022:1998, and AS/NZS 3548.

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

Power Line Emissions, IEC 61000-3-2: Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions.

Power Line Emissions, IEC 61000-3-3: Electromagnetic compatibility (EMC) - Part 3-3: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems.

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.

Installation and Repairs

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect 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).

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 document

This document, *Converged Communications Server Release 3.0 Installation and Administration* is developed for these reasons:

- Is a revision of the 2.x.x document
- Contains information about the new SIP Enablement Services, also known as Converged Communications Server
- Includes corrections of earlier information and newly developed information
- Presents additional information about SIP for the R3.0 Avaya Communication Manager system only. See the documents for Avaya Communication Manager for non-SIP issues.

This document is available online and in paper format. For your convenience, consider using the embedded cross-references to locate information. In addition, there is a table of contents and index for your reference. Online readers may also use the search facility of the software.

Audience

This document is for field technicians, remote service personnel, and user-assigned administrative personnel as a reference to configure and administer Avaya media servers using Communication Manager systems with SIP. We recommend having three to five years experience system administration, and experience with working on both media servers on the Communication Manager system and host servers in the SES system.

This document assumes that the engineer has a working knowledge of telecommunications fundamentals and PBX maintenance practices. This document also assumes that the system was installed and tested properly and brought into service with every fault cleared. Adjuncts and other devices external to the switch are covered by their own service documentation.

If you do not have these experiences and qualifications, please make arrangements for a mentor.

Document set

Although this book is published separately, it is part of a set. Use this document with the following references:

- Converged Communications Server or SIP Enablement Services documentation
- The SIP Personal Information Management document (SIP PIM)
- The Avaya Communication Manager administration document
- The Avaya Communication Manager Networking Connectivity document
- The Avaya Server Availability Management Processor (SAMP) Users Guide
- The Avaya Remote Supervisor Adapter (RSA) User's Guide

Hardware and Equipment

This book contains information about the equipment running SIP Enablement Services.

- Avaya S8300—for SES edge and home hosts servers
- Avaya S8500—for use as SES edge and home hosts and media servers. The S8500 has an RSA module used for remote servicing.
- Avaya S8500B—for use as SES edge and home hosts, and media servers. The S8500B has a SAMP module employed for remote servicing.
- Avaya S8700 media servers —for use as media server running Communications Manager
- Avaya S8710 media servers—for use as media server running Communications Manager
- PC or laptop
- Keyboard and monitor
- Null modem cable
- CAT 5 Ethernet crossover cable for duplexed hardware
- Extra NIC modules for duplexed hardware

Organization

- About this document, what you are reading now, gives general information on a SIP implementation, and how to use this document and others.
- Chapter 1: Introduction. This section describes the equipment running SIP Enablement Services, what it is, and what it does.
- Chapter 2: Overview of Changes to SIP Enablement Services. This section relates high-level information about SIP.
- Chapter 3: Shutdown procedures. Use this information to find out how to gracefully shutdown SES hosts.
- Chapter 4: Migrate hardware. Use this information to install the R3.0 version on new hardware.
- Chapter 5: Migrate software. Upgrade to the latest version of SIP Enablement Services software with instructions provided here.
- Chapter 6: Setup and configuration. Read this section if you need to configure a new SES host.
- Chapter 7: Installation procedures. This section gives separate install instructions for new, blank servers, for each type of hardware configuration.
- Chapter 8: Administration web interface. This section describes in detail the use and meaning of the screens in the administration interface.
- Chapter 9: Maintenance Web Interface. This section describes in detail the use and meaning of the screens in the maintenance interface.
- Appendix A: Licenses. This section presents an example of the text of the licenses you will need.
- Appendix B: Worksheet for Duplication. Use the worksheet here to help plan your install.
- Appendix C: Force All and Update All use and behavior. Use the worksheet here to help plan your install.
- Appendix D: SNMP Alerts. This section explains the SNMP alerts and how to correct them. An index of the SNMP trap names without the avSES prefix is included at the back of this chapter.
- Glossary provides explanations of abbreviations, acronyms, and terms.
- Index provides an alphabetical list of pertinent topics in this document. Under the **fields** heading, you can find all the screens a particular field resides on.

Conventions

Table 1: Explanation of typography

To represent...	This typeface and syntax are shown as...	For example...
commands	• Bold for **`commands`** • Bold italic for ***`variables`*** • Square brackets **[ ]** around optional parameters • "**|**" between exclusive choices	**`refresh ip-route [all	*location*]`**
screen input and output	• Bold for **input** • Constant width for `output (screens and messages)`	Set the **Save Translation** field to **daily**. The message `Command successfully completed` should appear.
Web interface	• Bold for **menu selections, tabs, buttons,** and **field names** • Right arrow **>** to separate a sequence of menu selections	Select **Alarms and Notification,** the appropriate alarm, and then click **Clear**. Select **Diagnostics > View System Logs**, then click **Watchdog Logs**.
Keys	Special font for **keyboard keys** and SAT screen **clickable buttons**	Press **Tab**. Click **Next Page**.

These conventions are used to:

- Physical dimensions are in English units [Foot Pound Second (FPS)], followed by metric units [Centimeter Gram Second (CGS)] in parentheses.
- Wire-gauge measurements are in AWG, followed by the diameter in millimeters in parentheses.
- Circuit-pack codes (such as TN790B or TN2182B) are shown with the minimum acceptable alphabetic suffix (like the "B" in the code TN2182B).

  Generally, an alphabetic suffix higher than that shown is also acceptable. However, not every vintage of either the minimum suffix or a higher suffix code is necessarily acceptable. The *Hardware Guide for Avaya Communication Manager (555-245-207)*, contains current information on circuit pack codes and functionality.

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 describes a situation that can result in harm to software, loss of data, or an interruption in service.

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

DANGER:
A danger statement alerts you to a situation that can result in harm to personnel.

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

Trademarks

Related resources

Table 1: Additional document resources, lists additional documentation that is available for you, some of which is referenced within this document.

Table 1: Additional document resources,

Document	Number
4600 Series IP Telephone R2.2 LAN Administrator's Guide	555-233-507
4600 Series IP Telephone R2.2 Installation Guide	555-233-128
4602/4602SW SIP Telephone Quick Reference	16-300471
4602/4602SW SIP Telephone User's Guide	16-300470
4610SW SIP Telephone Quick Reference	16-300473
4610SW SIP Telephone User's Guide	16-300472
4620/4621SW SIP Telephone Quick Reference	16-300475
4620/4621SW SIP Telephone User's Guide	16-300474
4600 Series IP Telephone R2.2 Document Library	16-300091
Avaya Communication Manager Capacities Table	555-245-601
online help for Avaya IP Softphone Release 5.x	---
online help for Avaya SIP SoftPhone Release 2.x	---
SIP Implementation Guide	16-300140
Administration for Network Connectivity for Avaya Communication Manager	*555-233-*504
Administrator Guide for Avaya Communication Manager	03-300509
Feature Description and Implementation for Avaya Communication Manager, Issue 3, May/June 2005	555-245-205
Avaya Extension to Cellular and OPS Installation and Administration Guide, Issue 9, May/June 2005	210-100-500
Avaya Extension to Cellular User's Guide, Issue 8, May/June 2005	210-100-700
Avaya Toll Fraud and Security Handbook	555-025-600
Converged Communications Server R3.0 *Installation and Administration*	555-245-705
	1 of 2

Table 1: Additional document resources, (continued)

Document	Number
Hardware Guide for Avaya Communication Manager	555-245-207
Quick Start for Hardware Installation: Avaya S8500 Media Server	555-245-701
Quick Start for Hardware Installation: Avaya S8700 Series Media Server,	555-245-703
Installation and Upgrades for the Avaya G700 Media Gateway and Avaya S8300 Media Server	555-234-100
Installing and Configuring the Avaya S8500 Media Server	03-300143
The Avaya Server Availability Management Processor (SAMP) User Guide	03-300322
Job Aids for Field Replacements for the Avaya S8500 Media Server	03-300529
Job Aid: Upgrading Firmware on the BIOS — Avaya S8500 Media Server,	03-300411
Maintenance Alarms Reference	03-300190
Maintenance Commands Reference	03-300191
Maintenance Procedures	03-300192
	2 of 2

Technical Assistance

Avaya provides the following resources for technical assistance:

- Within the U.S.
- International
- Downloading this book from the Web

Within the U.S.

For help with:

- Feature administration and system applications, call the Avaya 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.

Downloading this book 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 Acrobat Reader 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 publication date. The Avaya web site might also contain new product information and updates to the information in this book. You can download these updates.

Chapter 1: Introduction

This section describes Avaya SES R3.0, what it is and what it does. This general information is covered in these sections:

Converged Communications Server R3.0 Positioning Statement

The Converged Communications Server establishes the foundation for the Communication Services layer within the Avaya Communication Architecture. This layer unifies all enterprise real-time communications over an open SIP-based infrastructure, and provides the “glue” that binds with Avaya MultiVantage communication applications, exposing them as Web service components that can be easily invoked through standards-based clients or business applications, or as open APIs that provide a secure, reliable and highly scalable application development platform for access to Communication Manager services.

SIP Enablement Services and Application Enablement Services are modular offerings that can be ordered independently and implemented as needed by the enterprise on separate, dedicated industry-standard servers. In combination, the new services of the Converged Communications Server create an application environment that combines the loosely coupled multi-modal services and presence capabilities available via a SIP-based architecture with the open APIs that expose the full breadth of features and functions of Avaya Communication Manager.

The Converged Communications Server is a family of related product offerings that currently consists of two components:

- SIP Enablement Services
- Application Enablement Services

SIP Enablement Services

Avaya SIP Enablement Services R3.0 (SES) incorporates the SIP functionality previously introduced as Converged Communications Server Release 2.1, combined with new feature and scalability enhancements. The application combines the standard functions of a SIP proxy or registrar server with SIP trunking support and duplicated server features to create a highly scalable, highly reliable SIP communications network supporting telephony, instant messaging, conferencing, and collaboration solutions.

Application Enablement Services

Avaya Application Enablement Services 3.0 consolidate Avaya's existing application enablement assets – such as Communication Manager Application Programming Interface (CMAPI) and Avaya CT – into a single, Linux-based platform. This enables enterprises to leverage the tremendous variety of computer-telephony integration and interactive response applications developed for these interfaces. Application Enablement Services allow for powerful new applications to be written and deployed that fully leverage Communication Manager via standards-based APIs and Web service components.

Introduction to the Server

Find overview material about Avaya's servers that run SIP Enablement Services in these sections:

- SIP Enablement Services definition on page 24
- Data synchronization between Communication Manager and PPM on page 28
- How does this server fit into your system? on page 25

SIP Enablement Services definition

Avaya servers running SIP Enablement Services R3.0 perform proxy, registration, and redirection functions associated with SIP applications, such as Instant Messaging (IM). SIP is the Session Initiation Protocol, an endpoint-oriented, network messaging standard defined by the Internet Engineering Task Force (IETF). These Avaya servers are specifically referred to as Converged Communications Servers.

When SES hosts communicate with one or more Communication Manager R2.1 or R3.0 media servers, then the SES SIP proxy server supports communication among these elements:

- Non-SIP endpoints supported by Communication Manager:
  - Analog, DCP or H.323 stations
  - Analog, digital or IP trunks
- SIP-enabled endpoints not supported by Communication Manager:
  - Avaya SIP Telephones
  - Avaya SIP Softphone Release 2 and later

Advanced SIP telephony extends Communication Manager features to SIP-enabled endpoints.

SIP-enabled endpoints register with the Avaya proxy server. SIP-enabled endpoints can be managed by Avaya Communication Manager media servers as well. In addition, the SES edge proxy server supports the SIP-enabled instant messaging application between users of IP Softphone R5, and SIP Softphone R2 client software. For voice, the clients also must be logged in to and managed by Avaya Communication Manager media servers.

How does this server fit into your system?

In addition to the SIP Enablement Services servers, the support for SIP built into Avaya Communication Manager has the following attributes to help it fit into your system:

- It is built around open-source software and published standards (for example, Linux, SIP and H.323).
- It integrates traditional circuit-switched interfaces and IP-switched interfaces. This integration allows the customer to evolve from the current circuit-switched telephony infrastructures to next generation IP infrastructures, including SIP.
- It positions customers to leverage the increasing number and power of SIP-enabled applications, like Instant Messaging and presence.

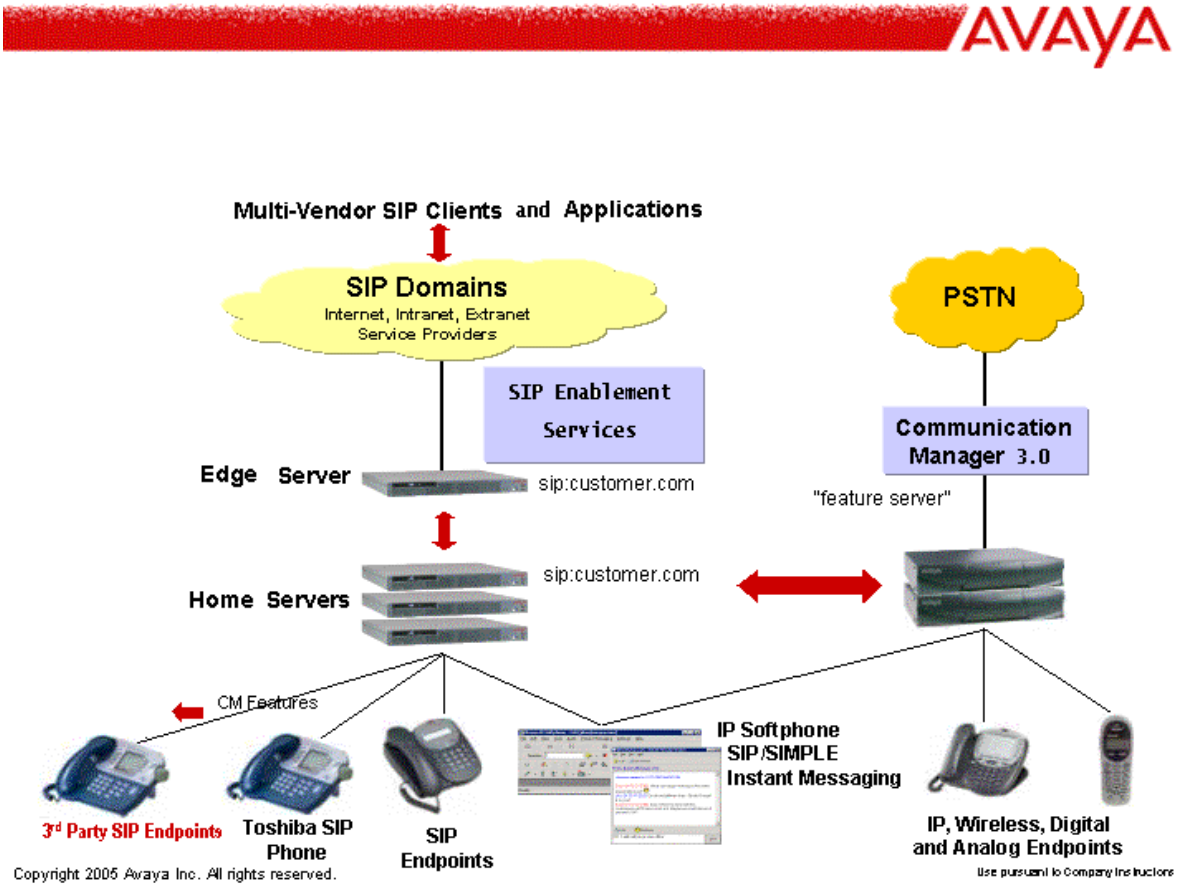
The modular and extensible system architecture that Avaya has chosen for offering SIP support has a unique benefit for Avaya customers: the set of features supported by SIP itself is augmented by those supported by Avaya Communication Manager. A Communication Manager media server becomes a telephony feature server, accessible from any SIP-enabled endpoint. This configuration provides access transparently to the many telephony features that the SIP standard currently does not address. Advanced SIP telephony provides value-added features such as bridging, three-party conference, unique ringing, and VIP calling.

System Architecture

Avaya's SIP architecture supports SES servers of different types, discussed in these sections:

System topography

Figure 1: Topography of system



Types of SES servers

There are several types of architectures using SES servers:

- Single edge server with a single home server
- Single edge server with many home servers
- A combined edge and home server

An administrator can change the authoritative domain of the network as necessary using the Master Administration interface.

An administrator can also migrate a combination home/edge server to distributed home and edge servers. Allow for any required data backups. In revision R3.0 of SES, backup both the Master Administration interface subsystem and the home system to back up all user data. Although administrators view SIP PIM data from the Master Administration interface on the edge, those data are stored on the home server associated with that edge server.

Edge servers

The edge server manages SIP requests from all domains, forwarding requests received from home servers. Along with the edge server, one or more home servers must also exist in this architecture. Only one edge server, or one combined home/edge server, is allowed for any one domain. For example, one edge server forwards requests to and from the `customer.com` domain.

Edge servers and combined home/edge servers may be duplexed for data redundancy.

Home servers

A home server manages SIP requests for the specific domain assigned for this server, and it forwards any requests pertaining to other domains to the edge server. One to 20 home servers and exactly one edge server is required in this scenario.

For example, a customer might have one home server for `A-users@company.com` and another home server for `B-users@company.com` within its network. Subdomains are not supported.

Home servers may be duplexed for data redundancy.

Home/Edge servers

A combined home/edge server contains software to act as both a home server and an edge server. This is a single-server scenario. No other home or edge servers may exist in this type of architecture.

End users are administered to one home only.

An home/edge combined server may be duplexed for redundancy.

Note:

Design your system architecture with scalability in mind. A migration to a new version may disrupt the database.

Data synchronization between Communication Manager and PPM

This section explains the circumstances under which dial plan data in Communication Manager propagates to the Personal Profile Management (PPM) database. This applies only to devices supported by SIP Enablement Services.

When a system administrator makes a change on Communication Manager and wants a telephone or device to implement that change, the administrator must use either the Master Administration interface or the SIP Personal Information Management (SIP PIM) interface to propagate the change to the device. Two scenarios illustrate this operation.

Scenario One

The system administrator makes changes to station data on Communication Manager for an extension that is associated with an end user, for example, add a button. For those changes to propagate to the phone, the administrator must perform these steps:

1. Log into the Master Administration interface.
2. Go to the **View Registered Users** screen.
3. Search for and identify the user.
4. Select the user whose phone configuration was changed on Communication Manager.
5. Select **Reload Configuration** from the drop-down menu at the bottom of the page.

Alternatively, either the administrator or the user may log in to SIP PIM for that user, go to the **My Devices** screen, and select **Reload Profile**. The user, however, is at a disadvantage at knowing when to do this.

Scenario Two

The system administrator makes a change on Communication Manager that would affect the dial plan. To propagate this information to the telephones, endpoints, or devices, the administrator must perform these steps:

1. Log in to the Master Administration interface.
2. Go to the **View Registered Users** page.
3. Search for and identify all the users.
4. Select all users on this home. Use the check box at the bottom of the page.
5. Select **Reload Configuration** from the drop-down menu at the bottom of the page.

Explanation

1. When the user or administrator selects either **Reload Configuration** from the Master Administration interface, or **Reload Profile** from SPIM, the Administration interface or the SPIM interface sends a message to PPM indicating the reload operation and the list of users to which it applies.
2. PPM collects common information from Communication Manager. Common information means anything that affects the dial plan, as well as station alias mappings. The system caches this information in PPM.
3. PPM notifies the event server, providing the list of users.
4. The event server sends out an event notification to each of the users, indicating the specific event in the avaya-ccs-profile package.
5. Upon receiving the notification, each device sends a `getEndpointConfiguration` request to PPM.

Administrative interfaces

All administrators gain access to SIP Enablement Services through a secure connection, that is, `https`.

Master Administration interface

The Master Administration interface is required to be installed on the edge server.

The Master Administration interface can add and delete users, and update data on all home or edge servers in a domain. The Limited Administrator interface cannot update user data.

The edge server updates all servers and their databases. For a combined home/edge server, these databases co-reside on a single node, and the home/edge cannot be used with additional home servers. The Master Administration interface supports administering both users and media server extensions. The Master Administration interface resides on the edge server (or the combined home/edge server). Only one server in the network may have the Master Administration interface. All other servers have the Limited Administrator interface.

Limited Administrator interface

The Limited Administrator interface cannot update user data. A home server with the Limited Administrator interface installed on it does not support administering users or their extensions, and cannot update the databases on other servers. With the limited interface you can administer maintenance items for the server, for example, and also view a list of registered SIP users on this home server.

Local redundant server feature

An optional feature in SIP Enablement Services is local failover as implemented by a pair of duplexed servers. This feature supports replicating the database and server software for any system node (home, edge, or combination home/edge). To take advantage of local failover, the servers must have a duplexed architecture. Read these sections:

- Duplex servers on page 30
- Server-level details of failover on page 31
- Local failover design on page 31
- Failover scenarios on page 31
- Causes for failover on page 32
- Server interconnections on page 33

Duplex servers

The local failover feature requires a duplex server configuration. For example, in a duplex configuration of edge servers, EdgeA has a backup server, EdgeB. Server Home1A has a backup of Home1B. EdgeB, Home1B are servers that take over should the A counterpart fail.

Because the failover feature is optional, both the simplex configuration supported in release 2.0.x and the duplex server configuration (2.1.x) are now supported in R3.0.

Duplexing of servers consists of a backup server for a stand-alone SES host, either home or edge. Duplexing requires the addition of dual NIC modules in both the primary and the backup server. Except for connection cables, no other optional hardware is necessary.

Not all the nodes in an enterprise's SES system need to be duplexed. You might choose one of the following architectures:

- Home/edge duplexed
- Edge with several homes, all duplexed
- Edge duplexed, homes simplex
- Edge simplexed, homes duplexed

In the last architecture, you may want one extra server. The extra server is not in use, but is set up and ready as a home server. You can quickly apply backed up data to it. Of course, timely system backups are mandatory.

Administrators can move a user from one home server to another using a drop-down list. When an administrator edits a user and changes their home server, the user is deleted from the first home's database and moved to the other home's database.

See Chapter 7: Installation procedures on page 67. The sections on duplex installations provide technical details.

Server-level details of failover

In this design, a server may be simplex or duplex. In a SIP Enablement Services system, a home or edge server may reside on two boxes, whose separate power, disk, and communications components make simultaneous failure unlikely. One box is the primary and provides service, while the other one (the backup or B server) monitors the primary server and takes over if it fails. The primary server performs extensive self-diagnostics as it recedes from service, voluntarily relinquishing control to the backup server in case it finds trouble. After giving up control (whether voluntarily or not), the primary server attempts to restore itself to a state in which it can provide service. Once this has been accomplished either automatically or with manual intervention, the former primary server then assumes the role of the new backup sever. In this way, the duplex-server configuration is maintained even after a local failover has occurred.

Local failover design

Elements within the design of Avaya's primary and backup servers and database local failover feature include:

- Health monitoring of the primary server
- Monitoring of the primary server by its backup server
- Mirroring on the servers of persistent data
- Recovery after failure of the primary server
- Monitoring of the control components so they do not contribute unduly to failures
- Restarting a failed processor, resynchronizing its database, and bringing it back into service as the backup server.

Failover scenarios

Typically, there are four scenarios in which an SES host may fail to process requests and provoke interchange:

- A primary server detects its own failure or a system administrator takes it out of service. A primary server will failover to the backup server, which becomes the primary server. This exchange of roles is called interchange. The server that was originally primary tries to become the backup server, restarting if necessary.

- A backup server fails or an administrator takes it out of service. In this scenario, no interchange between the two servers occurs. The primary server maintains normal operation without service interruption. The backup server may or may not successfully restart itself. if it does, it remains in the backup role.
- A primary server detects a communication problem with its request link. Communication data are shared by the two servers, and if the backup server detects no problem with its request link, then an interchange takes place. The server that had been primary restarts as the backup server.
- A backup server detects the loss of the primary server. It interchanges with the primary server, then tries to force the other server to restart as the new backup server.

Causes for failover

There are a number of reasons that a primary server might interchange with its backup server:

- The primary server cannot communicate with backup server using dedicated cable.

  If the primary server cannot communicate over the dedicated crossover cable to the backup server, but can communicate with the backup server using the main network IP LAN port. If the backup server can communicate back to the primary server, the backup server makes the interchange and become the new primary server.
- Data disk space is 90 percent full.
- One or more of the following server processes on the primary server is down:
  - Alarm process
  - Watchdog daemon
  - Heartbeat service
  - PostgreSQL service
- Logical IP addressing fails to operate.
- RAID 1 (disk mirroring) fails to operate.
- Any required system process on the primary server fails to respond to **mon** (monitor health).
- System cannot execute drbd (distributed redundant block device) for database replication.
- **`ipfail`**, a tool on the servers used to monitor IP network connectivity to their clients, reports an error on the local, primary machine but no error on its partner, the backup server.

Server interconnections

This section discusses several types of connections between the servers in the SES R3.0 system:

- Physical and logical connections on page 33
- Address Maps for Communication Manager and SES on page 33

Physical and logical connections

The most important aspect of interconnecting the servers is to have a clear idea of which server is the primary and the backup, and if the home and edge servers are combined or distributed.

When you install, check the instructions. Diagrams are provided for all network and power connections.

Address Maps for Communication Manager and SES

This section discusses address maps in SES 3.0.

- Address maps provide a way to handle messages to non-sip endpoints that are not in the SES user administration system, but are valid extensions in Communication Manager.
- They also provide a way for SES to direct a call that is unknown to appropriate Communication Manager or SES system for further routing.

SES can be used in an environment where only SIP trunking is needed. In this scenario, SES acts like a signaling gateway between the media server and the SIP service provider. In this configuration, there are two desired behaviors:

- SES routes all incoming calls from SIP service provider to the media server.
- SES routes all the calls from media server to the service provider.
- Communication Manager media servers that support SIP are Linux-based media server interface(s.)

These two behaviors are desired when a non-SIP user is calling in, or when a SIP user is calling outside the SES system to a non-SIP user. Address mapping in SES provides the necessary rules for routing to specific servers based on the patterns in the map.

The SIP exchanges between SES and Communication Manager are always over TLS. Address maps are often created to match SIP over UDP and SIP over TCP because many SIP end-points and proxies do not yet support SIP/TLS.

There are two types of address maps used by SES:

- Media Server Maps
- Host Maps

Media server maps route SIP messages to media servers running Communication Manager on one (or more) Linux-based media server interface(s)

Host maps route SIP messages to other SES hosts, devices, endpoints and any other place except Media Servers.

To define address maps, use these SES 3.0 screens:

- List Host Address Map screen
- Edit Host Contact screen
- List Media Server Extensions screen
- List Media Server Address Map screen
- Edit Media Server Address Map screen
- Edit Media Server Contaact screen

Become familiar with the fields and uses of the screens listed above. You should also be accustomed to using regular expressions for patterns, and the effect of wild cards.

Map

```
^sip:538[0-9]*@customer.com.*
```

In the example contact above,

^	matches the beginning of a line in the SIP message
sip:	denotes the protocol. This could be `sip:and sips:` protocols.
$	matches to a user identification
@	means a domain is next
123.4.56.255	is the domain or IP address of the URI
5060:	is the port number for tcp
transport = tcp	indicates transport method. For customer use, this must be **tls** on port 5061.

So in the example above, ^ matches the beginning of a line for any extension 3 or more digits in length, beginning with the digits 538, and ending with any other sequence of digits, in the customer.com domain.

Pattern

This is a Linux regular expression that will match the extension numbers you wish to map. Regular expressions are a way to describe text through pattern matching. The regular expression is a string containing a combination of normal text characters, which match themselves, and special metacharacters, which may represent items like quantity, location or types of character(s). (NOTE: You do not need to match punctuation like dashes, periods or parentheses which may sometimes be used to enhance the readability of telephone extensions.) For example, [0-9] represents any single digit and * represents any number of digits or characters. So the example in the preceding illustration
^sip:538[0-9]*@customer.com
would match any SIP invite message (^ matches the beginning of a line) for any extension 3 or more digits in length, beginning with the digits 538, and ending with any other sequence of digits, in the customer.com domain.

An example of a pattern useful for matching outside-call messages would be
^sip:9[0-9]*@customer.com
which would match a SIP invite message for any length of dial string beginning with the digit 9.

Square brackets contain a selection of characters to be matched, with a hyphen indicating a range; so in our example,[0-9] matches any digit, or for another example, [13579] matches odd-numbered digits. Curly brackets which contain a whole number match that number of instances of the preceding item. So for example, 538[0-9]{4} matches any seven digits beginning with 538. Note that the braces may require escape characters: \{4\}

Another helpful metacharacter is dot (period), which matches any single character; for example, the regular expression.* matches any quantity of any character(s).

For more information, refer to "*SIP Support in Avaya Communication Manager*", Doc ID 555-245-206.

Requirements for the SIP solution

These sections specify the required elements of the SIP Enablement Services R3.0 solution:

Hardware requirements

The server hardware required for an Avaya SES R3.0 server can be one of these:

- IBM e-server xSeries 305, referred to as S8500
- IBM e-server xSeries 306, referred to as the S8500**B**

IBM includes various CDs with its e-servers, including Director CDs, NetXtreme gE CD, eServer xSeries 305 CD, and Enhanced Diagnostics CD. These are ***not*** required to install an SES server. You must use the Avaya SIP Enablement Services Setup and Install CD.

An IBM Installation Guide is provided with the server, and includes instructions for installing these components:

- IBM Remote Supervisor Adapter (RSA) remote maintenance board (S8500 only).
- Dual in-line memory module (DIMM). ***This memory must be added before use.***
- Server Availability Management Processor (SAMP) remote maintenance board in S8500B machines.

A server that supports up to 3,500 users requires a total installed RAM of 1GB.

A server that supports up to 6,000 end users requires a total of 3 GB of memory. Because one edge can link to as many as 20 home servers, the edge should have 3 GB as well.

RAM requirements of 1GB or 3GB are required because RAM modules are deployed in pairs:

- 1GB = 2 512MB DIMMs
- 3GB = Two 512 MB DIMMs + Two 1GB DIMMs

Also, if your memory requirements are not fulfilled in your order, if you have to add memory from your own inventory, the speed of the DIMM modules must match. For example, if the server arrives with 333 MHz, any memory you add must be 333 MHz as well. Otherwise, the server will not even boot properly when you try to install. You might experience no video display, inability to eject the CD drive, and other odditites.

If you are installing a duplex system, install an additional, Intel ProShare dual Network Interface Card (NIC) in each server. For detailed procedures, see these documents:

- *Installing and Configuring the Avaya S8500 Media Server*, Doc ID 03-300143
- *Job Aid: Replacing the Dual Network Interface,* Doc ID 555-245-760

Avaya requires that one universal serial bus (USB) modem be connected to each server (one for each of the duplex servers) for remote access.

On the S8500, the modem is connected to the USB port on the server. On the S8500B, the modem is connected to the USB port on the SAMP card. An S8500 simplex server also requires a serial modem be connected to its RSA module. Multiple modems may be configured to share one analog phone line (each answering after a different number of rings). Implementation and maintenance services require remote access in this way.

The S8500 or S8500B server arrives with a blank, unpartitioned hard-disk drive, and without an operating system or any Avaya server software files installed. These components must be installed and configured properly before using SES. See the *RSA Users Guide* or the *SAMP Users Guide* listed in Related resources on page 20.

In addition, the IP connectivity must be configured correctly on all Avaya media servers running Communication Manager. For more details on configuring your IP system, refer to *Administration for Network Connectivity for Avaya Communication Manager,* Doc ID 555-233-504.

Software requirements

These software components are installed from the Avaya installation CD:

- Linux operating system
- WebLM, for managing licensing
- Proxy, IM Logger and TraceLogger services provided by Avaya
- PostgreSQL database
- Apache web server (for providing access to the Administration and Maintenance web interfaces)

See Appendix A: Licenses on page 437 to preview the licenses need for these software applications.

Chapter 2: Overview of Changes to SIP Enablement Services

This section summarizes the new and changed SIP features for SIP Enablement Services R3.0. These sections group material for you:

For your convenience, each summary directs you to the detailed descriptions of SIP changes and features.

Naming conventions

In this document, a decision was made to use the term SIP Enablement Services rather than Converged Communications Server to represent the product. See Introduction on page 23 for the explanation behind this.

In the screens, errors names, directory names and so on, most likely the reader will see CCS, even though, strictly speaking, the term should be SES, or SIP Enablement Services.

Call routing

SIP Enablement Services R3.0 implements Public Switched Telephone Network (PSTN) fallback. With this feature, if a call cannot be handled through the SIP domain, the home proxy sends it through the public switched telephone network via Communication Manager.

PSTN fallback requires either a host map or Communication Manager administration to operate.

Changes for administrators

- The administrator can add a user profile to the system that accommodates UNICODE (UTF-8) encoding. See Add User screen and Edit User Profile screen for more details.
- For any field in the Administration interface that supports UTF-8, the administrator can input Shift_JIS (AKA SJIS) as well. Whether the user's browser sends UTF-8 or SJIS is dependent upon the browser's language setting.
- The administrator can move a user from one home SIP server to another from the Administration interface. See Edit User Profile screen.
- A procedure is available for changing the DNS name without performing a full installation.
- Errors and their fixes are provided in an appendix.
- A compare and contrast discussion of the commands **Update All** and **Force All** is provided.
- Installation procedures are provided according to a specific hardware configuration.

Changing SIP domains and servers

- The administrator can change the SIP domain in the network. This is done at the Master Administration interface. See Edit System Properties screen on page 318, and Domain Access screens on page 319.
- The administrator can migrate a combined home/edge server to distributed, or separated, home and edge servers. A distributed architecture requires a data backup and might require a restore of the data. In SES, backup the Master Administration subsystem on the edge server *and* the home server to back up all user data.

Loading the authentication file

Local and remote access to SIP Enablement Services R3.0 Avaya Global Services login accounts is protected by Access Security Gateway (ASG) software that is included with installation CD. Attempts to log into these accounts are met with a one-time, random challenge string generated by ASG software. When Avaya Global Services personnel log in, Avaya connect tools automatically answer the ASG challenge with a valid response. Because of this automatic process, the secret keys for each server are not known by Avaya personnel.

A unique authentication file for each SES server is generated by Avaya during the installation process. This file contains the server's ASG secret keys. The Authentication File is encrypted when it is generated, and it remains encrypted when it is transmitted to the installer and after it is loaded on the SES server. Once it is loaded, the authentication file can be neither viewed nor deleted by anyone, but it can be replaced by a newer Authentication File. It can be decrypted and used only by ASG software.

Avaya personnel and business partners can obtain needed authentication files as part of the product registration process.

Avaya installers can access the Automatic Registration Tool (ART), which creates and download files with the ART script.

Business partners must call the RTS Database Registration Group, who provide either an e-mail or a download.

Once the authentication file is installed, all Avaya logins require either the appropriate password or ASG response, depending on which is specified in the file.

Screens

- The **List Users** screen has a **Select** list for the tasks to execute by user. Choose one user in the list by checking the box to the left of the screen. Tasks consist of the following:

  Contact List (new)

  Devices (new)

  Extensions

  Handles

  Memos (new)

  Profile

  Permissions (new)

  Watchers (new)

  The Delete button allows you to select more than one name.

  The **Move User** button lets you move a user to a different home. This button is available only if your system has multiple home servers.

  See the List Users screen on page 180.

- The administrator's **Contact List** screen is an administrative version of the Contact List screen in the SIP PIM interface. This includes the following screens: Contact Details, Group Details, Add Group, Update Group, Delete Group, Add Contact, Update Contact, Delete Contact, Speed Dial List, Watchers.

- The administrator's **Permissions** screen is an administrative version of the Permissions screen in the SIP PIM that manages the users' permissions.
- The administrator's **Devices** screen is an administrative version of the Devices screen in the SIP PIM. This screen is available only if the end user has a compatible device.
  - The administrator can view the **Terminal Information** for a device. Administration of the items below is performed by the end user directly on the device.
  - The **Tones And Volumes** screen is an administrative version of the Tones and Volumes screen in the SIP PIM for viewing the device's tones and volumes.
  - The **Ringer Settings** screen is an administrative version of the Ringer Settings screen in the SIP PIM for viewing the device's ringer settings.
  - The **One Touch Dial List** screen is an administrative version of the One Touch Dial List screen in the SIP PIM for viewing the device's one touch dial list.
- The **Add Host**, **List Hosts**, and **Edit Host** screen presents the minimum registration time in seconds, not minutes.
- The **Add Host**, **List Hosts**, and **Edit Host** screens include the following new fields:
  - Line Reservation Timer
  - Default Ringer volume
  - Registration Expiration
  - Default Receiver Volume
  - Profile Service Password
  - Default Ringer Cadence
  - Default Speaker Volume
  - Presence Access policy
  - Emergency Contact policy
- The **Registered Users** screen contains the following new tasks: Reload-complete, Reload-configuration, Reboot, and Status
- The **Registered Users** screen has a link for Apply task to all users and all on a home. Search for Registered or provisioned users.
- Emergency Contacts in the menu is a new item.

Chapter 3: Shutdown procedures

You may want to shut down the SES servers for the following reasons:

- Migration from an home/edge to distributed edge and one to many homes
- Migration from release 2.1 to release 3.0

You cannot directly upgrade SES servers from R2.1 to R3.0 using the **Software Upgrade** selection on the Maintenance web page. The graceful shutdown process shuts down simplex and duplex servers of any type and any hardware. Refer to the following sections:

- Best practices on page 43
- Shut down both servers in a duplex pair on page 43

Best practices

- In the URL address line of a browser, log in to the server you want to shut down to select it.
- Never use the Linux `stop` or `start` commands. Use the Maintenance interface shutdown procedures instead.
- In general, use Maintenance interface and switch over servers from primary to backup, and then issue a shutdown from the **Server>Shutdown Server** screen.

Shut down both servers in a duplex pair

This procedure applies to duplexed home or edge servers, either S8500 or S8500B.

By design, the server shutdown of a duplexed SES system follows the similar procedures as for Communications Manager.

Be aware that the **Shutdown Server** selection is not **Shutdown Entire System**. Shutdown Server just shuts a single server down.

1. Start a web session to the backup server using its physical IP address, or name.
2. Select **Busyout Server** at the Maintenance web page.
3. Make sure the backup server in the duplexed pair is out-of-service now by checking the Maintenance Server Status web page.

4. Keep the primary server in service. Select **Status Summary** of the Maintenance web page for the information.

   On the **backup server**, the Status Summary screen should look like this:

```
                              SERVER STATUS


                    sv11

             Mode: Out of service
    Major Alarms: yes
    Minor Alarms: yes
 Server Hardware: okay
       Processes: okay


                sv12
             Mode: Active (Unknown)
```

   The **primary server** shows the Status Summary as follows:

```
                              SERVER STATUS


                    sv12

             Mode: Active (In service Primary)
    Major Alarms: yes
    Minor Alarms: yes
 Server Hardware: okay
       Processes: okay


                sv11
             Mode: Active (Out of Service)
```

5. Click **Shutdown Server** on the Maintenance web page.

   Shutdown Server has a check box for a restart option. To shut down the server and leave it down, leave the check box empty.

   On the **primary server**, the Status Summary now displays the status as below:

```
                              SERVER STATUS

                    sv12

             Mode: Active (In service Primary)
      Major Alarms: yes
      Minor Alarms: yes
    Server Hardware: okay
          Processes: okay


                 sv11
               Mode: Inactive (Unknown)
```

6. If you want to shut down the remaining primary server, then start a new web session to the primary server and click **Shutdown Server**.
7. Manually restart the two servers by power cycling.

   On an S8500B, you may need to unplug the RJ11 connection and plug it back in to cycle the power to the SAMP.

   The Status Summary page shows that the backup server is out of service because of the earlier busyout action.
8. To bring the duplex servers back to service, manually restart both servers with a power cycle.
9. Log in using a valid user ID and password.
10. To verify a successful reboot, run the **statapp** command on both servers.

The primary server should have all these services as shown:

```
root@sv12> statapp
Watchdog       16/16 UP
TraceLogger    04/04 UP
INADSAlarmAgen 01/01 UP
CCSTrapAgent   01/01 UP
GMM            05/05 UP
SNMPManager    01/01 UP
ImLogger       04/04 UP
SipServer      40/40 UP
EventServer    55/48 UP
MtceMgr        06/01 UP * 6
drbdEventSvc   06/01 UP * 6
```

```
mon             06/01 UP * 6
SME             08/08 UP
```

The backup server should have these services up:

```
Watchdog        15/15 UP
TraceLogger     04/04 UP
INADSAlarmAgen  01/01 UP
CCSTrapAgent    01/01 UP
GMM             05/05 UP
SNMPManager     01/01 UP
ImLogger        00/04 DOWN
SipServer       00/40 DOWN
EventServer     00/48 DOWN
MtceMgr         06/01 UP
drbdEventSvc    06/01 UP
mon             06/01 UP
SME             08/08 UP
```

11. On the backupserver's Maintenance web page, select **Release** to set the backup server to be the primary server **(In Service Backup)**.

Chapter 4: Migrate hardware

Migrate an existing hardware configuration

This section describes the tasks involved in upgrading a CCS 2.x installation to SES R3.0 software. See Setup and configuration on page 61 to prepare to install a new server, and read these sections:

- Migrating from an R2.x home/edge to an R3.0 edge with several homes on page 48
- Migrating from simplex to duplex 2.x on page 50

Best practices

- For this release of SES, the implementation of SES R3.0 on a CCS 2.x.x platform is considered a migration and not an upgrade.
- If you have a combined home/edge architecture, use the Maintenance interface and backup all datasets on that server. If you have a distributed edge with one or more homes, perform a full backup for the edge and each home separately.

  Recall that SIP PIM data are stored on the home server, and viewed using the Master Administrator interface on the edge server.
- Use the Maintenance interface for backup and capture all user data. Then the server boots from the Avaya SES software CD and the hardware is prepared to receive the new software.
- After files have been installed and the server rebooted, you may run the **`ccsInstaller`** script.
- Every execution of the ccsInstaller script requires that you answer all questions. You cannot make a change to a particular question and then cancel out of the script. After answering all questions, ccsInstaller executes several more scripts to update all the files requiring these changes. After a new database is created and initialized, restore the user database you saved.
- For assistance, contact RTS Tier III to preserve the database.
- If you are migrating with a duplex pair, reboot the server after the ccsInstaller script has completed running. Rebooting is not necessary if you execute ccsInstaller on a simplex machine.

Migrating from an R2.x home/edge to an R3.0 edge with several homes

Use these steps:

1. Backup the data on the 2.1 version servers to a different drive.
2. Install a new, blank server to act as a distributed home server. See Chapter 6: Setup and configuration on page 61 on how to get set up.
3. On the SES R3.0 server, backup all datasets on the home/edge server to a remote server. Use FTP as provided on the Backup maintenance screen.
4. Run **`ccsInstaller,`** and specify on the new home server, a new IP address for the new home server. Specify that the server not run the Master Administration database. Avaya recommends that edge servers run the Master Administration interface.

   If you re-execute the ccsInstaller script, you must respond to all of its questions again. You cannot make a change to a particular question and then cancel out of the script.

   After you answer all the questions, ccsInstaller executes several more scripts to update all the files requiring these changes.

   If you are migrating with a duplexed pair, reboot the server after ccsInstaller script has completed running. Rebooting is not necessary if you execute ccsInstaller on a simplex machine.

5. If the new home server is a simplex, start the server by answering **y** to the last prompt of ccsInstaller script: Do you want to start the server now? y/n (**y**).

   If the new home server is part of a duplex pair, follow the procedure to bring up the duplex system beginning with Step 7 in Shut down both servers in a duplex pair on page 43.
6. Using the Maintenance interface on the new home server, stop these services:

- proxy
- imlogger
- eventserver

   a. On a simplex server, select **Stop** for each of the processes listed on the Services web page in the Master Administrator interface.

   b. On a duplex, stop the services as follows:

      1. HTTP to the backup server's Maintenance web page, and busy-out the backup system.
      2. On the primary server, stop each of the services by clicking Stop on the Services web page of the Master Administrator interface.

7. On the existing home/edge server, stop these services:
   - proxy
   - imlogger
   - event server

   a. On a simplex server, select Stop for each of the processes listed on the Services web page in the Master Administrator interface.

   b. On a duplex server, stop the services as follows:

      1. HTTP to the backup Maintenance web page, and busy-out the backup system.
      2. On the primary server, stop each of the services by selecting **Stop** on the Services web page in the Master Administrator interface.
8. Using the **List Hosts** screen in the Administrator interface, perform **Migrate Home/Edge**
9. Enter the IP address of the new home server created in Step 4 of this procedure.
10. Enter the database password.
11. Select **Submit** to start the migration.

    Continuing with the Migration performs a Force All operation automatically. With Force All, data are pushed from the edge server to all of the administered home servers.

    Now, the former combined home/edge server becomes the edge. The user data from the edge server is moved to the new home server created in Step 4.
12. On the new home server, using the Master Administration interface, recreate the non-standard system administrator user accounts and the WebLM license file on the SES R3.0.
13. On Communication Manager, busyout the sip trunk, change the far-end node name from the home/edge server to the new home server's name, and release the sip trunk.
14. Start the services proxy, imlogger, and eventserver on the edge and the new home:

    a. On a simplex server, select **start** for each of the services listed on the Services web page.

    b. On a duplex server, start the services as follows:

       1. On the primary, start each of the service by clicking on the **start** on the Services web page.
       2. HTTP to the backup server's Maintenance web page, and release the backup system.
15. Change the PPM address on all the Toshiba Business Phones (TSP).

    If the TSPs were registered previously, they register automatically to the new home server and can make calls.
16. Choose a license source as described on Server license installation on page 103, for example.
17. Once the migration is complete, additional home servers may be added to the configuration.
18. Reboot if this is a duplex configuration.

Migrating from simplex to duplex 2.x

This procedure converts a single CCS edge server running release 2.1 on an S8500 hardware platform over to a duplexed edge server for failover capabilities. This high level document is for administrators that have a thorough understanding of installing and configuring the previous version of Converged Communications Server.

This is not a detailed explanation of the procedure.

CAUTION:
Do not use this procedure on S8500B hardware.

Best Practices

- Read through the entire procedure before beginning the reconfiguration.
- Read the install instructions for a system configuration like this one.
- Avaya assumes no responsibility for lost data or configurations.
- Moving from a simplex configuration to a duplex pair is a system re-configuration that takes place as you work through the questions in the ccsInstaller script.
- The backup of the OS and Security datasets of an R2.1 server should not be restored to a 3.0 server. Only the backup of the user database of R2.1 can be restored on the 3.0 server.

Backup existing server

Use these steps:

1. Backup data on a separate drive.
   a. Maintenance Page -> Backup Now – Select User Data, Server and System Files, and Security Files.
2. Backup via FTP.
   a. The backup must be off the CCS system you are replacing and should be off the CCS solution.
3. Check the Backup history to verify the backup was successful.
   a. Backup History – Select Radio button for the correct **Backup** and **Check Status** – should read BACKUP SUCCESSFUL for all 3 files.

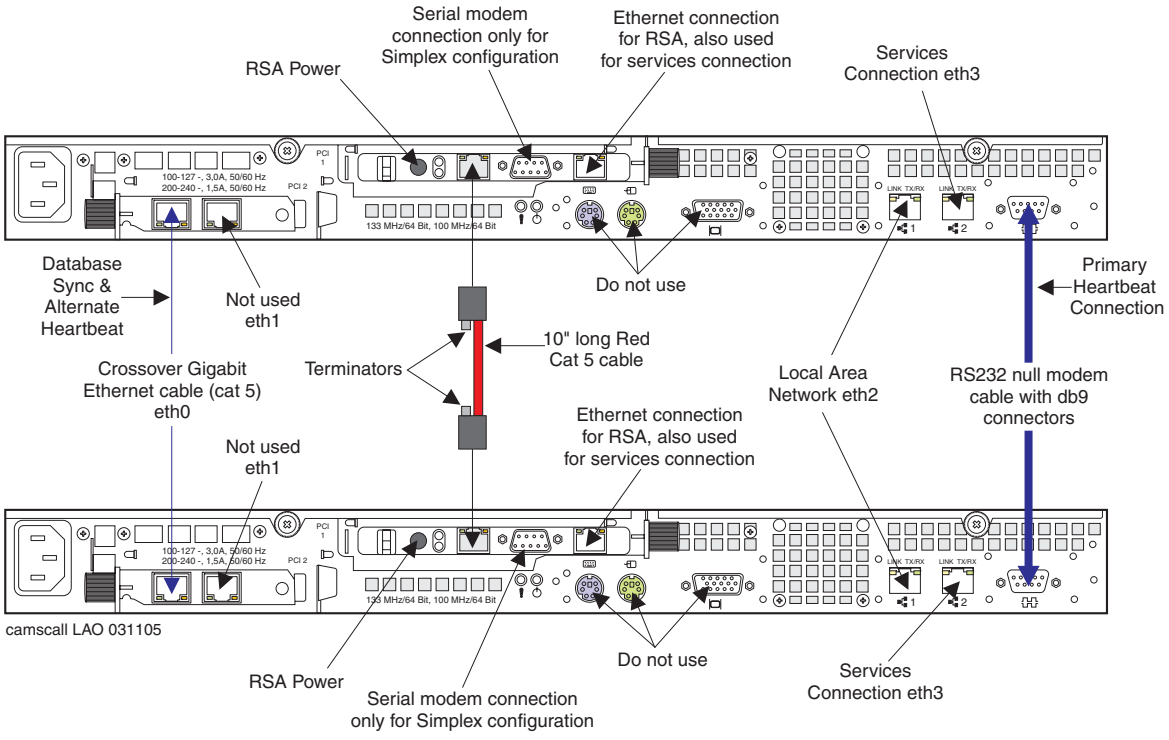
Install new hardware

Use these general steps to install a new, blank server:

1. Power system down and remove cover.
2. Install new NIC – Be certain the NIC is properly seated.
3. If not already added, also install additional RAM on “new” 305.
4. Replace cover.
5. Power up RSA card (upgrade if necessary).
6. Telnet into RSA to verify User and Password (192.11.13.6).
   a. USERID/PASSW0RD or craft/password.
   b. Refer to RSA documentation if needed.
7. Complete all physical connections.

   See Figure 2.

Figure 2: Port locations and connections for S8500 duplex



Install software

Note:

The “old” physical IP address *must* be the “new” logical IP address. If not, the entire database will be corrupt and unusable.

Use these steps:

1. Load the installation CD and run the **ccsInstaller** script on server A – complete install of High Availability option.
2. Load the installation CD and run the **ccsInstaller** script on server B – complete install of High Availability option.
   a. Import the original database using the View/Restore Data item of the Maintenance interface. You may need to check the box for **Force restore if server name mismatch** on the **View/Restore Data** results page. Probably the new server name is different from the name of the original single box.
   b. Create and load new license based on the new MAC address in use.
   c. Verify that the license host address on **System Properties** page is the physical IP address of the server on which the WebLM application is running.
      - Restart the sipserver process on all home servers through the start/stop proxy.
      - On each host click **Services** (on Administration interface under Media Servers).
      - Click **Stop proxyserver**.
      - Click **Start proxyserver**.
   d. Change physical connections for the modem and ring patterns
      - The simplex uses a Y connector to split between the USB and RSA modems. In a redundant scenario, use the Y connection to split between 1 USB modem on each box. The number of rings on B must be changed to 5 rings to differentiate between the servers.
3. Contact Tier III or Tier IV engineer to make above modem change and for latest updates, patches, or limitations for a new redundant system.

Chapter 5: Migrate software

Migrate an existing software installation

This section describes the tasks involved in upgrading an R2.x installation to R3.0 software. See Setup and configuration on page 61 to prepare to install a new server.

- Migrating from SES R2.x to SES R3.0 on simplex servers on page 54
- Migrating from SES R2.x to SES R3.0 on a duplexed pair on page 56
- Migrate a duplex home/edge from SES R2.x to SES R3.0 on page 58
- Migrate a duplexed edge with distributed duplex homes on page 59

Best Practices

- The implementation of R3.0 on a 2.x.x platform is considered a migration.
- If you have a combined home/edge architecture, use the Maintenance interface and backup all datasets on that server. If you have a distributed edge with one or more homes, perform a full backup for the edge and each home separately. Recall that SIP PIM data is actually stored on the home server, and only viewed using the Master Administration interface on the edge server.
- Using the Maintenance interface will capture all data. Then, the server boots from the Avaya ccsInstaller CD and the hardware is prepared to receive the new software. After files have been copied and the server rebooted, you may run the ccsInstaller script and begin administration of the server.
- Every execution of the ccsInstaller script requires that you answer all questions. You cannot make a change to a particular question and then cancel out of the script. After answering all questions, ccsInstaller executes several more scripts to update all the files requiring these changes. After a new database is created and initialized, restore the user database you saved.
- For assistance, contact RTS Tier III to preserve the database.
- If you are migrating with a duplex pair, reboot the server after the ccsInstaller script has completed running. Rebooting is not necessary if you execute ccsInstaller on a simplex machine.

Migrating from SES R2.x to SES R3.0 on simplex servers

It is important to note that if this migration fails, reinstall R2.x and restore all the backups. User data from the edge server and any home servers are restorable without having to reinstall the entire database.

The backup of the OS and Security datasets of the existing CCS R2.1 server should not be restored to the R3.0 server. Only the backup of the user data, the database, of R2.1 can be restored on the R3.0 server.

Migrate to R3.0 with these steps.

1. On the R2.x server, backup all datasets to a remote server. Use FTP as provided on the **Backup** maintenance screen.

   Verify that the backup ran successfully by going to the Backup History web page.

2. Make a note of all non-standard administration accounts on the SES server. These accounts can be listed on the SES server by going to **Server Configuration->Admin Accounts**. These accounts will have to be manually re-created on the server following the upgrade.

3. Run **`ccsInstaller`** on each of the servers in the configuration. Do not start services or provision any data on the systems yet.

   When you re-execute the ccsInstaller script, you must respond to all of its questions again. You cannot make a change to a particular question and then cancel out of the script. After you answer all the questions, ccsInstaller executes several more scripts to update all the files requiring these changes.

   Reboot after running ccsInstaller. Do not provision the new system. Data will be provisioned using the Restore feature of the interface.

4. Restore user data *only* with the **Restore** web page. Do not restore any OS data or security data.

5. Accept the default login and password. Administer all non-standard administrative accounts that were noted in Step 2.

6. For each administered Host on the **List Hosts** page edit its host information and, administer a new **Profile Service Password** for each host.

7. For each administered media server on the **List Media Servers** page, edit the media server information and administer the following fields:
   - CM Login
   - CM Password
   - CM Confirm password
   - Profile Service Password
   - CM FQD name or IP Address
   - SMS FQD name or IP Address
8. Follow the procedure for re-installing the licenses for the system.
9. Enable WebLM from the System Maintenance pages.
10. Perform a Force all from the **List Hosts** page when all systems are running the same software version.
11. Reboot all servers. Rebooting all servers will start all system services.
12. Choose a license source as described on Server license installation on page 103, for example.

Migrating from SES R2.x to SES R3.0 on a duplexed pair

This procedure describes performing a software upgrade on duplex servers.

The backup of the OS and security datasets of the existing CCS R2.1 server should *not* be restored to the SES R3.0 server. Only the backup of the user data, database, of R2.1 can be restored on the R3.0 server.

Recreate the system administration user accounts using the Administration web pages and the WebLM license file on the R3.0 server.

When you re-execute the ccsInstaller script, you must respond to all of its questions again. You cannot make a change to a particular question and then cancel out of the script. After you answer all the questions, ccsInstaller executes several more scripts to update all the files requiring these changes.

To summarize, this procedure consists of doing a fresh 3.0 install on your current hardware, and then do a data restore. Then, visit the pages and fill in the fields that are new to R3.0. After this, bring the servers into service

Use these steps:

1. HTTPS to the logical server using the logical IP address of the logical server.
2. Go to the **Maintenance** web interface.
3. Go to the **Status Summary** web page and find the backup server.
4. HTTPS to the backup server using the physical IP address of the backup server.
5. Go to the **Maintenance** web interface.
6. Go to the Shutdown Server screen on page 368 web page and busy-out the backup server.
7. Follow the Download Files instructions to download the tar file for the new release.
8. Visit the Edit Hosts screen and set these fields:
   - DB password
   - Profile Service Password
   - Presence Access Policy
   - VMM fields are optional
9. Visit the Edit Media Server screen and set these fields:
   - CM Login and password
   - CM FQD name or IP Address
   - SMS FQD Name or IP Address
10. After the software upgrade is completed, submit the request for **Make Upgrade Permanent**.

11. Restart the server using the **Shutdown Server** web page with the **Restart Server** box checked.
12. After the server is completely restarted, go to the Maintenance interface to release the backup server.
13. HTTPS to the logical server using the logical IP address of the logical server.
14. Go to the Maintenance web interface.
15. Go to the **Interchange Servers** screen to perform an interchange.
16. Make sure that the two servers have interchanged their roles as a duplex pair successfully.
17. Recreate the system administrative user accounts using Administration interface and the WebLM license file using the administration interface.
18. Reboot the server after ccsInstaller script has completed running.
19. Repeat Steps 1 through 18 to upgrade the new backup server.

Migrate a duplex home/edge from SES R2.x to SES R3.0

Note that moving from a simplex configuration to a duplex pair is a system reconfiguration, that is, new IP, domain name, and so on.

The backup of the OS and security datasets of the existing CCS R2.1 server should not be restored to the SES R3.0 server. Only the backup of the user data, the database, of CCS R2.1 can be restored on the SES R3.0.

If you re-execute the ccsInstaller script, you must respond to all of its questions again. You cannot make a change to a particular question and then cancel out of the script.

After you answer all the questions, ccsInstaller executes several more scripts to update all the files requiring these changes.

Use these steps:

1. Follow Steps 1 through 18 in Migrating from SES R2.x to SES R3.0 on a duplexed pair on page 56 to complete a software upgrade on the duplex home/edge.
2. HTTPS to the logical IP address of the duplex home/edge.
3. Go to the Master Administration interface, List Hosts web page.
4. On the Hosts screen, select **Update All** or **Force All** to synchronize the databases on the hosts.

   For details on the use of Update All and Force All, see the appendix Force All and Update All use and behavior on page 471.

Migrate a duplexed edge with distributed duplex homes

Upgrading the software on a duplexed edge server with distributed duplex home servers starts on the duplex edge servers first, followed by upgrading the home servers.

The backup of the OS and security datasets of the existing R2.1 server should not be restored to the R3.0 server. Only the backup of the user data, the database, of R2.1 can be restored on the R3.0.

If you re-execute the ccsInstaller script, you must respond to all of its questions again. You cannot make a change to a particular question and then cancel out of the script. After you answer all the questions, ccsInstaller executes several more scripts to update all the files requiring these changes.

Use these steps:

1. Start the installation from the edge server first.
2. Complete the steps 1 to 12 in Migrating from SES R2.x to SES R3.0 on simplex servers on page 54 to upgrade the software on the edge server.
3. HTTPS to the logical IP address of the duplex edge server.
4. Go to the List Hosts web page under the Master Administration Interface.
5. Repeat Steps 1 through 12 on all the home servers. Choose a license source as described on Server license installation on page 103, for example, on all the home servers.
6. After all the home servers have been upgraded successfully, HTTPS to the logical IP address of the duplex edge server.
7. Go to the List Hosts screen of the Administration interface.
8. On the Hosts screen, select **Update All** or **Force All** to synchronize the databases on all the hosts.

   For details on the use of Update All and Force All, see the appendix Force All and Update All use and behavior on page 471.
9. Reboot all servers in this duplex configuration.

Chapter 6: Setup and configuration

Use the information in this section before beginning any installations. This information is pertinent to all install procedures.

Configuring a new server

This section describes installing an Avaya SIP Enablement Services R3.0 for the first time. These instructions apply to an Avaya media server S8500 or S8500B for use as a home/edge, distributed edge, distributed home, simplex or duplex.

For an expert installation without troubles, expect about one hour per server.

See Migrate hardware on page 47 for an R2.1 to R3.0 migration. Perform these tasks:

- Back up your data if needed.
- Perform Initial assembly and setup on page 61.
- Loading the authentication file on page 62
- Read Best practices for installing on page 64.

Initial assembly and setup

All SES servers must be properly connected and configured on an enterprise's IP network.

For an S8500 media server, you must have these documents to install memory, and to verify or update firmware:

- *Upgrading Software and Firmware—Avaya S8500 Media Server,* Doc ID 555-245-111
- *The Avaya RSA User's Guide*, Doc ID 555-245-702
- *Job Aid: Replacing the RSA*, Doc ID 555-245-759

For an S8500B media server, you must have this document to add memory and verify version numbers:

- *The Avaya Server Availability Management Processor User's Guide*, Doc ID 03-300322

For endpoints on Avaya Communication Manager to interoperate with SES servers, SIP trunking must be administered first in Communication Manager. Refer to the document *SIP Support in Avaya Communication Manager* for more details. This administration includes, but is not limited to, specifying these values:

- Network names of all proxy hosts on the IP Node Names screen
- Home Domain assigned to server(s) on the IP Network Region screen
- Appropriate Proxy Selection Route Pattern on the Locations screen
- SIP trunk group members on the **System-Parameters Customer-Options** screen

Likewise, for a SIP station to work through Communication Manager, the same thing has to be administered.

For information on IP network assessment and readiness testing, refer to *Administration for Network Connectivity for Avaya Communication Manager*, Doc ID 555-233-504.

For a list of needed information, meaningful examples, and answers to the questions in the install script, see Worksheet for Duplication on page 461. Be sure you have all the information needed for your site before you begin to install.

If you install used or refurbished equipment, make sure that it has been erased completely, and that it matches exactly the new equipment it represents.

Loading the authentication file

Local and remote access to SIP Enablement Services R3.0 Avaya Global Services login accounts is protected by Access Security Gateway (ASG) software that is included with the installation CD. Attempts to log into these accounts are met with a one-time, random challenge string generated by ASG software. When Avaya Global Services personnel log in, Avaya connect tools automatically answer the ASG challenge with a valid response. Because of this automatic process, the secret keys for each server are not known by Avaya personnel.

A unique Authentication File for each SES server is generated by Avaya during the installation process. This file contains the server's ASG secret keys. The Authentication File is encrypted when it is generated, and it remains encrypted when it is transmitted to the installer and after it is loaded on the server. Once it is loaded, the Authentication File can be neither viewed nor deleted by anyone, but it can be replaced by a newer Authentication File. It can be decrypted and used only by ASG software.

Avaya personnel and business partners can obtain needed authentication files as part of the product registration process.

Avaya installers can access the Automatic Registration Tool (ART), which creates and download files with the ART script.

Business partners must call the RTS Database Registration Group, who provide either an e-mail or a download.

Installing the authentication file

Once the authentication file is acquired, the installer navigates to the Authentication File web page in the SES maintenance interface.

1. Log into the Administration interface top page and select the Maintenance Web Interface.
2. Find the Security heading in the left column and click Authentication File.
3. If the authentication file is present in the FTP directory, chose the box **Install the Authentication file I previously downloaded**.
4. If the authentication file is elsewhere, such as on the installer's laptop, choose the box **Install the Authentication file I specified below** and enter the file path or URL to the authentication location of the authentication file.
5. Click **Install**.

   The page displays either a successful installation message or an error message.

   If there is an error, click on Help at the top left of the page to display context-sensitive help.

Once the authentication file is installed, all Avaya logins require either the appropriate password or ASG response, depending on which is specified in the file.

Check your work

To ensures that the RFA license and ASG authentication file are installed and that alarming is configured, perform these tests:

- For license files, log into the **Administration** interface and go to **Server Configuration**-->**Manage Licenses** screen. The screen displays the installed licenses for each host server.
- If the ASG authentication file is installed and working, the sroot account is set up, and your attempts to log in as superuser (su) from the Linux shell are challenged by ASG.
- Check Alarming with the `testinads` command in the Linux shell. This command generates a test alarm to the telephone number and/or SNMP INADS IP address assigned in alarm configuration.

Best practices for installing

These are high-level concerns about what you need to do before and during an install:

- Find out if you are installing S8500 or S8500B hardware.
- Determine if the home and edge servers will be on one machine (combined) or on separate physical machines (distributed).
- Do hardware set up first, than do all software tasks.
- Ascertain if any of the servers have a backup machine cabled directly to it, creating a duplexed pair.
- Install the Master Administration interface on the first edge server you install.
- In a duplex configuration, be clear on the names and roles of which physical server is A and which is B. The designation A and B *do not* indicate which machine is primary and which is backup.
- In a duplex configuration a second NIC must be installed in A and B.
- In a duplex configuration, there is a preferred order. Install the A server first and the B server next.
- Do not perform SIP trunking on the Communication Manager until SES servers are ready.
- When administering a duplexed pair, the instructions in this document are provided in the correct order. You are directed to install and administer the edge first, then install and administer homes, then administer Communication Manager media servers.
- If you use an S8500 server, obtain an RSA password and login.

  If you have an S8500B server, no password is required for the SAMP module.
- Recall that when using S8500B servers for a duplexed pair, the eth ports are eth1, eth2 and eth3. In a simplex configuration of an S8500B, the eth port is eth0.
- Also note that when using S8500 servers for a duplexed pair, the employed eth ports are on the second NIC, eth0 and eth1, and on the motherboard, eth 2 and eth3. In a simplex configuration of an S8500, the motherboard eth ports are eth0 and eth1.

Checklist

Here is a checklist to give you an overview of the install procedures. Details can be found in the rest of this document.

_____Verify that the Communication Manager media server is installed and functioning properly before you begin.

_____Take receipt of server, make sure no damage has occurred en route, and unpack.

_____Assemble hardware.

_____Install additional memory for greater than 3000 users.

_____Install additional NIC card in a duplexed configuration.

_____Connect cables correctly for your site.

_____Power cycle and check power on self test.

_____Decide the function of your machines:

home, or edge, or home/edge

_____Decide role of this machine:

primary or backup

_____Find the procedure you need in Chapter 7: Installation procedures on page 67.

_____Connect a laptop to the server.

_____For a duplexed system, disable console redirection.

_____Verify the server's firmware and BIOS.

S8500 is A61. S8500B is A24. BIOS Build ID:KEEH21AUS BIOS Release Date: 06/18/04.

_____Verify the remote maintenance board's firmware:

RSA on an S8500 is PLET08A, PLEH08B, or PLBH08B.

SAMP on an S8500B is AVAYA_1_0_SP1_BUILD_11.

_____Boot from the CD and answer the questions as directed.

_____Run the ccsInstaller script and answer the questions.

_____Load the Authentication files as described on Loading the authentication file on page 40.

_____Install an edge server first, and the edge backup if present.

_____Install every home server.

_____Bring to in service state.

_____Work through each server's Setup screens:

Setup SIP Domain with Edit System Properties screen

Setup Hosts with Add Host screen

Edit Default User Profile

Add Media Server

_____Work through each server's Maintenance screens:

Set Time and Date screen

Configure Server screen

Authentication File screen

_____Run `checkconfig` after putting in service.

_____Verify the software installation.

_____Administer hosts, both homes and edges, using the Administration interface.

_____Administer licensing from the maintenance chapter.

_____Verify licensing with the Maintenance interface Authentication File screen.

_____Set up the Communication Manager media server for use of endpoints with the SES hosts.

_____Test with calls.

_____Test interchangeability from primary to backup if necessary.

Chapter 7: Installation procedures

This section provides installation steps for installing SIP Enablement Services on fresh, new SES servers. A separate procedure is provided for each configuration.

To use the procedures in this section:

- Determine the hardware platform you have, either an S8500 or S8500B.
- Determine the host configuration, either combined or distributed.
- Find out if this is a duplex or simplex installation.

Based on these three criteria, locate the correct install procedure.

- Installation tasks must be performed locally by an Avaya or Business Partner installer.
- Work through the installation procedures sequentially, on one server, unless otherwise instructed.
- First install the server that will have the Master Administration software installed in it. This server is always the edge server.
- After installing any other edge servers, install all home servers.
- In a duplex pair, install server A first as the primary server. Next install Server B as the backup server. Be sure you have a clear understanding of which is which to answer the installer script questions correctly.
- When administering machines, administer the edge server first. Then do the home servers.

Installing SES R3.0 on an S8500B

The SES servers that receive the install CD are home servers and an edge server. A SIP domain has only one edge server, disregarding it's backup, and that edge can support up to 20 home servers.

These instructions explain how to install SES home and edge hosts that use an S8500 in these configurations:

- Installing an S8500B combined home/edge—simplex on page 68
- Installing an S8500B combined home/edge—duplex on page 85
- Installing an S8500B simplex edge—duplexed homes on page 107

Installing an S8500B combined home/edge—simplex

Follow the procedures here to install a single, combined home/edge server that has no backup server.

Best Practices

- Do not use any form of the Linux **`stop`** or **`start`** commands.
- Review the information on connections and relate it to your own hardware installation

Connection schema

Before beginning the installation procedure, check all connections and make the physical connections correctly.

Table 2 shows the port and purpose for an home/edge simplex configuration.

Important:
If you check the Ethernet port mappings with `ifconfig`, your command output will match the information in the table. If you use a different method, perhaps a web page, your results will differ from what is listed in the table.

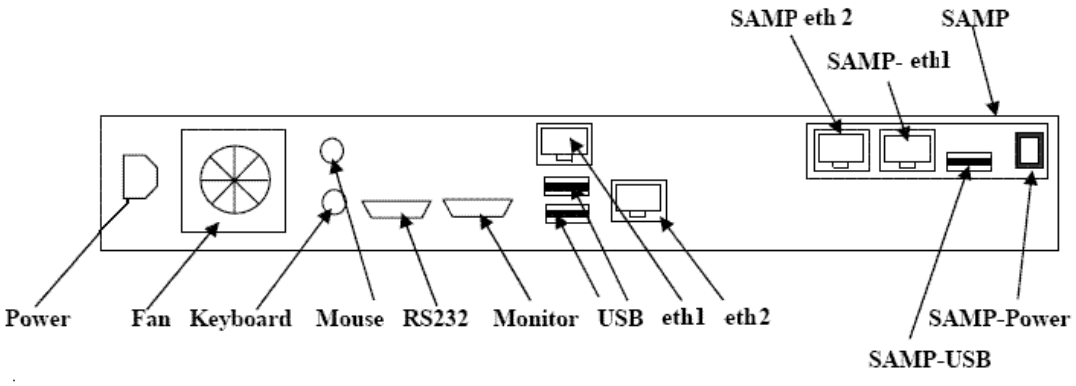
At this point in the installation, the SAMP ethernet ports do not display.

Table 2: S8500B combined home/edge simplex ethernet port address assignments

Ethernet Port	Purpose
S8500B motherboard eth1	Connect to customer's LAN
S8500B motherboard eth2	Reserved for Avaya Services
SAMP eth1	Reserved for Avaya Services
SAMP eth2	Unavailable. Connects SAMP to motherboard internally

Figure 3 shows a single S8500B port configuration with a single SAMP card installed.

Figure 3: S8500B Port Diagram—simplex



Note:
No additional NIC is required for a simplex configuration.

See Figure 4 for a photograph of the S8500B backplane for your reference.

Figure 4: S8500 backplane with SAMP card

Follow these steps:

1. Take the S8500B server out of the shipping box and check for damage.
2. Verify that all the required hardware and cabling are present.
3. Ensure that all server components are seated properly.
4. Connect a power cord to the server and the SAMP module.
5. Connect the Services laptop PC to the SAMP.
6. Run the command **`ifconfig`** at a prompt to verify connectivity. If connectivity is incorrect, you will need to escalate the problem.

Verify firmware and BIOS on the S8500B server

This procedure checks the S8500B server.

The laptop should be on, the server should be off.

1. Connect the laptop PC to eth 2 on the server.

   Alternatively, you may use an RS232 cable to connect to the server.

2. With your browser, make sure that the laptop is not configured to access the internet.

   In MS Internet Explorer for example, click **Control Panel** > **Network Connections** > **Local Area Connections**, and select **TCP/IP**. If necessary, change the IP address so that the laptop performs as a console and does not try to attach to the Internet.

3. From the laptop control panel, open a HyperTerminal session.

   Start > All Programs > Accessories > Communications > Hyperterminal

4. Connect a power cord to the S8500B at this point, not earlier.

5. Power up the S8500B and observe the boot messages in the HyperTerminal window.

   The system immediately prompts for BIOS information.

6. Press F1 quickly.

7. Choose **System Summary** and check that the extra RAM has been properly installed and enabled.

   The server should have either 1 gigabyte or 3 gigabytes, depending on the size of the user base. See Hardware requirements on page 36.

8. Choose **Devices** > **IO Ports** > **Primary Master** and verify these BIOS settings:

   a. Verify that the BIOS is set so that the **CD drive** is the first choice of system boot device.

   b. Verify that the server has been upgraded to the minimum Avaya BIOS or an approved later release. There should be BIOS Date and EEPROM fields on the screen. For the S8500B, the minimum version is 21A or greater. To check the BIOS version, follow these steps:

      - Select **System Information** > **Product Data**.
      - There should be BIOS Date and EEPROM fields on the screen.
      - In the EEPROM field, look for a value similar to KEEH**21A**US.

        The notation **21A or 24A** designates the BIOS version. If the BIOS version is earlier than 21A, upgrade the BIOS firmware.

        See *Upgrading firmware on the BIOS—Avaya S8500 Media Server*, document ID 03-300411, for instructions.

Load the install CD

This procedure copies application files to the server and creates file systems.

Use these steps:

1. Set the IP address of the laptop or PC to 192.11.13.5 and use a netmask of 255.255.255.252.

   You do not need to specify a default gateway.

   Use a CAT 5 cross-over cable between the ethernet ports of the laptop and the home/edge server.
2. Put the R3.0 install CD in the CD drive and close.
3. Turn off the power to the server.
4. Cycle the AC power to restart the server by.

   Allow the server to boot from the CD, and wait about 3 minutes.
5. From the laptop, connected to eth 2, start a telnet session to the server you are installing.

   a. In the first window, select this item:

   `- Install or Upgrade CCS Software`

   b. In the second window, select this item:

   `- Release Version CCS software load number`

   Wait about 10 minutes for this to complete.
6. Press **Enter** to accept each of the default settings.

   Accept these defaults to install a new release on this server.
7. Select **y** or Enter to proceed.

   The server copies the software Redhat package managers to the appropriate partition.

   The server ejects the CD from the drive and reboots. The reboot disconnects the terminal emulator's session with the server.

   If the CD does not eject, you must restart the installation procedures.
8. If the CD ejects correctly, wait three minutes for the reboot to complete.

   You might use **`ping -t`** to alert you when the reboot is complete.
9. When the Avaya Services port is ready again, start up a telnet session, and log in using standard procedures.
10. If prompted to suppress alarm origination, accept the default of **y** for yes, suppress alarms.
11. Run the command **`ifconfig`** at a prompt to verify connectivity of the eth connection of eth 1 and eth 2.

    If connectivity is incorrect, fix it or escalate the problem.

Verify firmware on the SAMP module

Perform this portion of the installation on every server in your configuration. Ignore any warnings or errors.

This part of the install checks and does the first update of the SAMP module.

Verify the SAMP's firmware after loading the CD.

1. Start a terminal session to the server you are installing, either telnet or ssh, and then type `sampupgrade`.

   If the version of SAMP firmware is up to date, then `sampupgrade` output is as follows:

   ```
   craft@lzccsSamp> sampupgrade
   ==>SAMP FW: AVAYA_CCS_1_0_SP1_BUILD_11 [OK]
   craft@lzccsSamp>
   ```

   If the SAMP firmware is incorrect, the upgrade operation starts automatically. Output is shown below.

   ```
   ==>Update SAMP FW [kernel-0.0109-root-0.0109] to [samp-update-
   AVAYA_CCS_1_0_SP1_BUILD_11.tbz]
   ==>Update SAMP w/ the factory configuration
   ==>Update SAMP for [factory] configuration
   ==>Sync SAMP configuration XML: /usr/hap/etc/avaya109.xml
   ==>Configure eth2(192.11.13.6) device at SAMP
   ==>Wait for the SAMP to reboot with the factory configuration.
   [0]
   ==>Run sampfixer to upgrade SAMP FW now
   Notes:
   SAMP update takes few minutes to complete.
   After firmware upgrade is done, enter "Y" at the
   "Commit [Y|N]" prompt to commit the new firmware.
   The CCS Server will be rebooted at the end.
   ==>Remove /var/home/ftp/pub/samp-update-*.tbz
   ==>Install SAMP FW: /usr/hap/etc/samp-update-
   AVAYA_CCS_1_0_SP1_BUILD_11.tbz
   ==>Synchronize the server's IP address with the SAMP's
   ==>Update SAMP firmware now
   ```

```
Warning: Permanently added 'my-samp,10.221.248.1' (RSA) to the
list of

known hosts.

1723+1 records in

1723+1 records out

mke2fs 1.27 (8-Mar-2002)

.

.

.

Correct: [y|n] y

The SAMP accepted the new firmware and is rebooting.
```

Run ccsInstaller script

In this section, run the ccsInstaller once to complete the SAMP upgrade in Verify firmware on the SAMP module on page 73. When complete, run ccsInstaller again to assign names, addresses, and roles to the server.

1. Login and type **`ccsInstaller`** to run the initial configuration script.

   The ccsInstaller script checks the SAMP firmware version and upgrades it if necessary. If the SAMP firmware is running the correct version, ccsInstaller continues. Otherwise, ccsInstaller displays warning messages indicating the current firmware version of SAMP, and then indicating what the correct version should be. The ccsInstaller stops. If ccsInstaller stops with this warning, run the **`sampupgrade`** command to upgrade the SAMP firmware.

   SAMP upgrade takes place automatically, but works the same as in the previous upgrade. This time it will not take as long.

2. When the SAMP upgrade is finished, type **ccsInstaller** again.

- You may want to use the information in Worksheet for Duplication on page 461 to help you answer the prompts in this section.

  After you answer all the questions, ccsInstaller executes several more scripts to update all the files requiring these changes.

  - The ccsInstaller script prompts you for network settings of the SES server:
    - Host name
    - Fully qualified domain name
    - Host IP
    - Network mask
    - Default gateway
    - DNS IP, and so on

3. Select **OK** after you have entered these.
4. Enter the information listed under Setup and configuration on page 61.
5. For the prompt **High Availability configuration option**: answer **n**. This is a simplex installation.
6. Enter information for initial database setup for the postgreSQL service, such as an mvss password.
7. Choose an mvss database password. This password is required for initial database administration or future troubleshooting.

   Note the several status messages regarding the database account, both before and after the following steps. After those messages, web services restarts.

8. For the prompt **Are you initializing a Master Administrator on this machine**, enter **y**.
9. For the prompt **Start Services**, answer **y.**

Verify the Avaya server software installation

Perform this procedure on all machines in your configuration. These steps verify that the software can run. Later, you or another person might do a more complete installation check before the customer performs their own customer acceptance testing.

1. After the Avaya Services port is ready again, log in using standard procedures.
2. Use the **`statapp -c`** command to verify that SES services are running.
3. If the processes sipserver and eventserver are not running on your simplex SES host, either check the troubleshooting document for your software, or contact your Avaya representative.
4. If the status of these processes shows **partially up**, wait a few moments and check again. The partially up status indicates a transition.

   The status of all processes should show UP ***except*** the status of sipserver, eventserver and imlogger. The status of sipserver, eventserver and imlogger stay Partially Up and change to UP after the administration is completed.
5. Press **Control C** to quit the statapp command.
6. Set the time and date at the system prompt with the Linux **`date`** command.

Initial administration for home/edge server

The hardware is databased through ART. Once administered, the passwords you set here, and PPP address are provided through ART after the installation.

- Select UPDATE on each screen as you work through it.
- The script guides you through the steps to administer this information.

Follow these steps:

1. From your browser, go back and set the laptop to connect to the internet and not act as a dumb terminal to the server.
2. Open a web browser window and type the following in the URI field:

   https://*hostname*/admin

   or

   https://*ipaddress*/admin

   The *hostname* is the fully qualified domain name of the server if you have DNS administered.

   If you do not type **/admin**, the SIP PIM interface for the end user displays.
3. Enter the default administrative user name in the **Logon ID** field and press Enter.
4. Enter the initial password for the admin account, and select **Logon**.

   Note that after this initial logon, the default password should be changed for security reasons. See Change Administrator Password screen on page 328.

Use the Maintenance interface

At this point, you are logged in through the customer LAN as shown in the connectivity diagrams.

In the Maintenance interface, perform these tasks:

1. From the log in screen, choose **Maintenance** Interface,
2. Select **Server > Server Date and Time**.

   Set the time and date with the Maintenance page Server Date/Time screen on page 369.
3. Select **Server > Server Configuration > Configure Server**.

   Synchronize the time with an external time source. See Network Time Server screen fields on page 376.
4. Select **Server Configuration > Configure Server >** and view all the screens there. Be sure that the fields show the correct data for your site.

5. Remain in the **Security > Authentication File** screens and make sure all the fields are correct.

   This step is related to the authentication files you downloaded in the pre-installation preparation discussed in Loading the authentication file on page 62.

6. Close that browser and open the main page showing Administration and Maintenance interface choices.

Use the Administration interface

At this point, you are still accessing the application from the customer LAN connection. In the Administration interface, perform these tasks:

1. Select **Launch Administration Web Interface**.

   You receive a warning about License Error Mode. You may ignore it until after completing the server installation.

2. Select **Setup** to display the first of the Setup screens on page 159.

   Select each link on the **Setup** screen to complete the initial host administration screens.

3. Select **Setup SIP Domain**. The system displays the Edit System Properties screen on page 318.

   a. Enter the network name or IP address of the SIP domain to which this home/edge server is assigned (usually, an enterprise's top level) in the **Domain** field.

   b. In the **License Host** field, enter the host name or fully qualified domain name of the home/edge server.

   c. Select **Update** and then select **Continue**.

4. From **Setup**, select **Setup Hosts**.

   a. On the Add Host screen on page 165, enter the name of the server, for example, edge.customer.com, in the **Host Name** field and select **Home/edge** from the entries in the drop-down list **Host Type**.

   b. In the **Password** field, enter the mvss database password that you set during installation Step 7 in Run ccsInstaller script on page 75.

   c. Set up the **Profile Service Password** for the server.

      This password provides permissions between the SES hosts, both home server and edge server.

      The Profile Service Password is not used by users or administrators. Rather, it is a password that uniquely identifies a proxy for intra- and inter-proxy communication. The Profile Service Password must be unique for each administered host.

d. Set **Listen and Link protocols**

The only link protocol supported for SIP trunking in Avaya Communication Manager is TLS. By default, the system shows all listen protocols and one link protocol (TLS, for SES host-to-media server communication). You may select your own, so long as any link protocol you select is also selected as a listen protocol.

For example, if you are using a 46xx SIP telephone, or if you are connecting to a SIP service provider, then you could check all three listen protocols. If you are using only the IM client in IP Softphone R5 or SIP Softphone R2 within your enterprise, then the TLS Listen Protocol is sufficient.

e. (Optional) When a SIP client tries to register with this host, by default the minimum-duration registration acceptable is 15 minutes. If you wish to change this value, enter a new, whole integer, 900 through 59,940, in the **Minimum Registration** field.

f. (Optional) You may accept or change the defaults for the following fields:

- Presence Access Policy
- Minimum Registration (seconds)
- Outbound Routing Allowed From
- Outbound Proxy
- Outbound Port
- Outbound Transport
- Outbound Direct Domains

g. Select **Add** and then select **Continue** on the confirmation screen.

h. Select **Update**. All pending updates administered on this host become synchronized on all other hosts.

5. (Optional) Select **Setup Default User Profile** to access the Edit Default User Profile screen on page 172
6. Select **Setup Media Servers** to display the Add Media Server screen on page 174. You must do this step before any media server extensions can be administered.

   After these associated screens have been completed, **Setup** disappears from the left-hand menu of choices.
7. Select the Hosts screen, select **Update All** or **Force All** to synchronize the databases the databases.

   For details on the use of Update All and Force All, see the appendix Force All and Update All use and behavior on page 471.
8. Change the default password at the top login window for security reasons. See Change Administrator Password screen on page 328.

Server license installation

Perform this procedure on the edge server only.

An SES home/edge server requires these licenses:

- Home proxy license
- Edge proxy license
- Home seat licenses

These three licenses are accommodated in one file.

Terminology differs between the Master Admin interface License screen and the WebLM->Licensed Products->IMPRESS screen. See Table 3.

Table 3: License Terminology

Admin Web Interface	Web LM screen
Edge Proxy	Edge Proxy License (EDGE_proxy)
Basic Proxy	Home Proxy License (BASIC_proxy)
Home Seats	Home Seat Licenses (HOME_seats)

The WebLM server is installed in one location only, on an edge server. For a duplexed pair, pick an edge server's physical name or IP address, usually the A server.

Obtain licenses for the Avaya SES system with these steps:

1. To obtain the correct MAC address, go to a command line and type `get-mac-address`.

   Alternatively,

   a. Enable and log in to WebLM using steps 5 through 9 below.

   b. Select **Server Properties**. The contents of the **Primary Host ID** field is the eth0 MAC address of the server.

2. Use your established RFA web procedures for obtaining licenses for Avaya servers.

   a. Use the MAC address you obtained in Step 1.

   b. Go to the RFA web site at http://rfa.avaya.com and download the license file to where you can upload it later on, typically to a location on the PC used by authorized services personnel.

3. You must logon and select the link to the Maintenance Web Interface.
4. From the list of available Security screens, select the link to view the WebLM Software screen.
5. If WebLM is not already enabled, select **Enable WebLM**.

6. From the list of available Security screens, select the link to view the WebLM License Administration screen.
7. Select **Access WebLM**.

   The system displays the WebLM application screen.
8. From the WebLM screen, select **License Administration** and then enter the WebLM default administrative password.
9. After your initial log in, the system prompts you to change the password. WebLM logs you out and expects you to log back in with your new password.
10. Select **Install license**.
11. Then select **Browse** and navigate to the location where you saved the license file in Step 2, and then select Install.

    The proxy server will renew acquired licenses every 5 minutes. However, initially, it has not acquired any licenses (there were none installed) so the proxy server will actually be trying every 60 seconds. Then, once it gets them all, it will renew them every 5 minutes.
12. If you need a server to acquire or re-acquire a license immediately, perhaps to update the number of home server seats you are allowed quickly, use these steps:

    a. Restart an Avaya proxy server manually.

    b. From the Master Administration interface, select the **Services** screen, and then select the proxy server's **Stop** link.

       Confirm that this process has stopped, and select the **Start** link.

Administer Communication Manager and endpoints

At this point you are about three-quarters done. For this portion, get a copy of the document *SIP Support in Avaya Communication Manager*. You will need the administration steps there.

Endpoints for Communication Manager include a variety of devices, terminals or stations:

- Avaya SIP phones
- Third-party SIP phones
- Wireless, digital, and analog endpoints
- Avaya 46xx Softphone
- SIP Softphone R2 or later
- IP Softphone R5 or later
- Before your installation is complete, you must use the established procedures to administer the Communication Manager media server for use with SIP. These steps include adding users of SIP telephones and Avaya SIP Softphones, adding extensions for each user, and updating proxy route patterns, as appropriate.
- A SIP-enabled station, such as the Avaya 46xx, should be administered in Communication Manager 3.0 as an Off-Premises Station (OPS). See the *Avaya Extension to Cellular and OPS Installation and Administration Guide*, Issue 6 or later.

Follow these steps:

1. Administer Communication Manager to work with SIP devices.

   The fields that differ SIP from non-SIP Communication Manager media server setup are detailed in *SIP Support in Avaya Communication Manager*.

   The document includes entries for Signaling Group and Trunk Group setup that are specific to SIP. After you have completed setup in Communication Manager, perform a **Save Translations** to save changes.

2. Set up the telephones and endpoint devices.

   After setting up Avaya SIP Softphone users in Communication Manager as SIP Softphones on (OPTIM/OPS), ensure each client PC has the proper release of Softphone software installed, licensed and configured to use SIP for Instant Messaging (IM). Refer to online help in the SIP Softphone application for more information. You also may wish to verify that these softphones can register with the edge/home, and then can send and receive instant messages, update their contact lists, and so on.

3. Check the endpoint devices

   After administering SIP telephones in Communication Manager, ensure that each telephone has a version of firmware that can support SIP. Note that the Avaya 46xx SIP telephone ***requires*** that you enter a domain name on its SIP Settings page. You may wish to make and receive test calls, too.

For application notes on which third-party SIP endpoints are supported, go to the web site:

`http://www1.avaya.com/enterprise/resourcelibrary/applicationnotes/` and then select the link for **Network Infrastructure** under **DevConnect Product Integration**.

Installing an S8500B combined home/edge—duplex

Follow the procedures here to install a combined home/edge server with a backup combined home/edge.

Best Practices

- Do not use any form of the Linux **`stop -a`** or **`start -a`** commands on a duplexed server. For SES servers, these commands are disabled.
- Review the information on connections and relate it to your own hardware installation
- Go through all the procedures on the primary server, server A. Then repeat the needed procedures for the backup server, server B.
- Always start installation of duplex systems on the A server.
- When installing the A server, the B server is powered down.
- After installation for the primary server, server A, is completed, leave the A server on.
- Power on the B server and perform the installation on the B server.

Connection schema

Before beginning you installation procedure, connect and then check all physical connections.

Table 4 shows the port and purpose for an home/edge duplex configuration.

Important:
If you check the Ethernet port mappings with **`ifconfig`**, your command output will match the information in the table. If you use a different method, perhaps a web page, your results will differ from what is listed in the table.

At this point in the installation, the SAMP ethernet ports do not display.

Table 4: S8500B Ethernet Port address assignments

Ethernet Port	Purpose
S8500B eth0	Connect to customer's LAN
S8500B eth3	Reserved for Avaya Services
S8500B eth1 on NIC	Connects Server A:192.11.14.10 to Server B:192.11.14.11
S8500B eth2 on NIC	Not Assigned
S8500B eth4	Unavailable. 192.11.13.1 Connects host and SAMP S8500B
SAMP eth1	Unavailable. 192.11.13.2 Connects SAMP to host internally
SAMP eth2	Connect to other SAMP eth2 with terminator cable.

Figure 5 shows the port numbering for an S8500B duplex configuration, which is different from the numbering on an S8500B simplex configuration.

Figure 5: S8500B Port locations for duplex pair

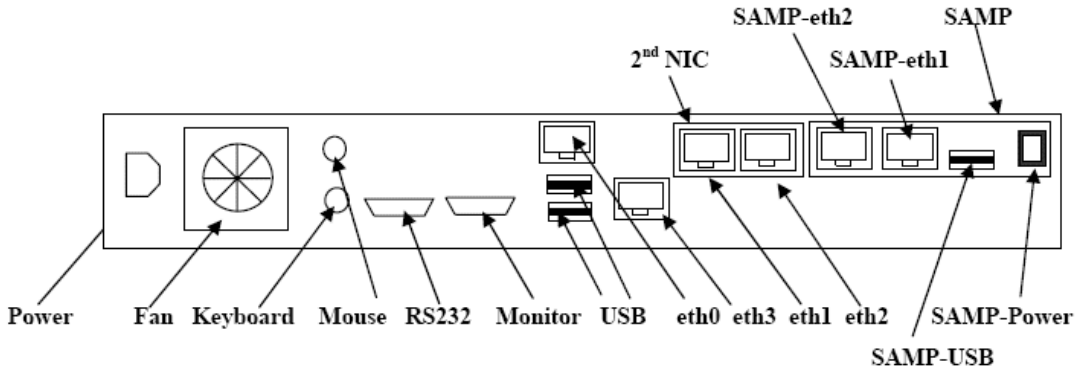
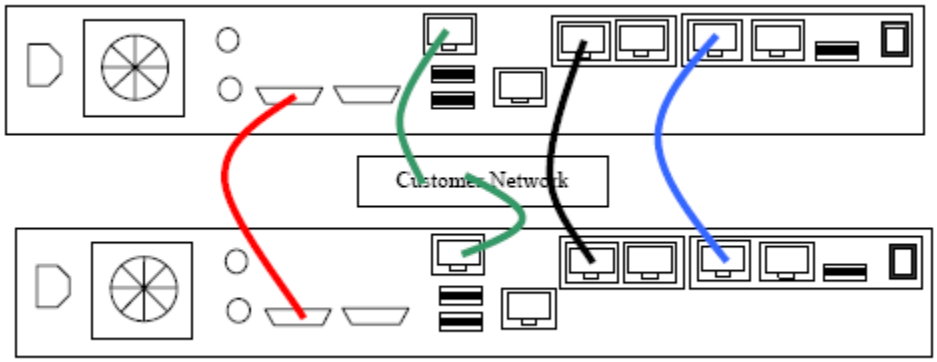


Figure 6 shows how the duplexed pair should be connected.

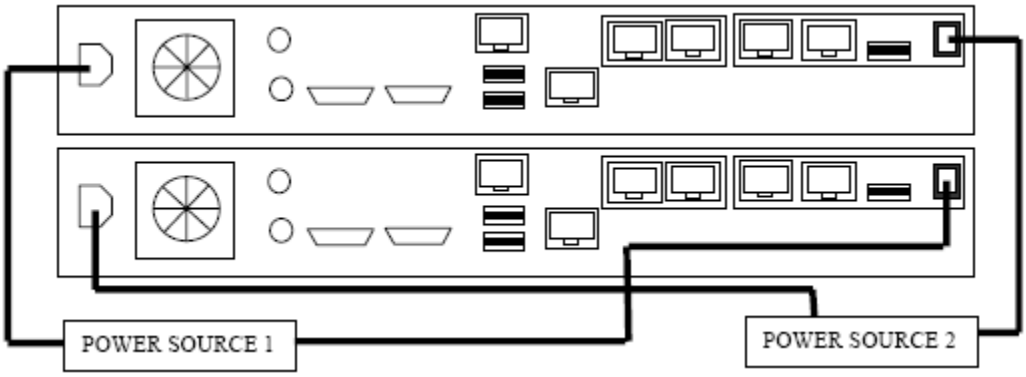
Figure 6: S8500B Duplex connections



- Red - Heartbeat. Null Modem Cable connects both RS232 ports
- Green - Customer Network connection. (S8500B Ethernet port eth0)
- Black - Data Link. Cross-connect LAN cable (S8500B Ethernet port eth1). Connects the motherboards
- Blue - Control Link. Cross-connect LAN cable (SAMP Ethernet port eth2). Connects the SAMP cards.

Figure 7 shows the power connections for the server itself and the SAMP module. Make sure your power cabling is correct.

Figure 7: Power connections for a duplexed pair of S8500B



Disable console redirection

Obtain a keyboard and monitor to connect to the serial port and perform this procedure on only the server A.

1. Verify that all the required hardware and cabling are present for all servers.
2. Take the server out of the shipping box and check for damage.
3. Ensure that all components are seated properly.
4. Connect a power cord, console, and keyboard to the server.
5. Power up the server.
6. The system immediately prompts the BIOS information on console.
7. Press F1 now.
8. You may have a short-timing window here.
9. You may need to hold down the F1 key to assure that the system displays the BIOS setup page.
10. Select **Advanced Setup**.
11. Select **Console Redirection**.
12. Select **COM port address**.
13. Use the arrow keys to change to **Disabled**.
14. Save changes and exit the BIOS configuration screen.

    The server reboots.

For any other procedures, see:

- *Installing and Configuring the Avaya S8500 Media Server*, Doc ID 03-300143 page 49,
- *Job Aid: Replacing the Dual Network Interface,* Doc ID 555-245-760

Verify firmware and BIOS on the S8500B server

Perform this procedure on both the server A and server B.

1. From the lap top, open a HyperTerminal session.
2. Connect a power cord to the S8500B at this point.
3. Power up the S8500B and observe the boot messages in the HyperTerminal window.
4. The system immediately prompts for BIOS information.
5. Press F1.

   Check that the extra RAM has been properly installed and enabled in the BIOS.

   The server should have either 1 gigabyte or 3 gigabytes, depending on the size of the user base. See Hardware requirements on page 36.

6. Verify these BIOS settings:
   - Verify that the BIOS is set so that the CD drive is the first choice of system boot device.
   - Verify that the server has been upgraded to the minimum Avaya BIOS or an approved later release. There should be BIOS Date and EEPROM fields on the screen. For the S8500B, the minimum version is 21A. To check the BIOS version, follow these steps:

     a. Using the arrow keys to navigate, select **System Information**.

     b. Select **Product Data**.

     c. There should be BIOS Date and EEPROM fields on the screen.

     d. In the EEPROM field, look for a value similar to KEEH21AUS

     21A or 24A designates the BIOS version. If the BIOS version is earlier than 21A, it is necessary to upgrade the BIOS firmware.

See *Upgrading firmware on the BIOS—Avaya S8500 Media Server*, Doc ID 03-300411, for instructions.

Load the install CD

This procedure copies application files to the server and creates file systems.

Perform this procedure on server A first and then server B. Keep the backup server powered off while working with the active server. Keep the server A on while working on server B.

Use these steps:

1. Set the IP address of the laptop or PC to 192.11.13.5 and use a netmask of 255.255.255.252.

   You do not need to specify a default gateway.

   Use a CAT 5 cross-connect cable between the ethernet ports of the laptop and the home/edge server.
2. Put the SES R3.0 install CD in the CD drive and close.
3. Turn off the power to the server and cycle the AC power to restart the server by.

   Allow the server to boot from the CD, and wait about 3 minutes.
4. From the laptop, connected to eth 3, start a telnet session to the server you are installing.
   a. In the first window, select this item:
      - **Install or Upgrade CCS Software**
   b. In the second window, select this item:
      - **`Release Version CCS software load number`**

      Wait about 10 minutes for this to complete.
5. Press Enter to accept of each default setting.

   Accept these defaults to install the new release on this server.
6. Type **y** or Enter to proceed.

   The server copies the software Redhat package managers to the appropriate partition.

   The server ejects the CD from the drive and reboots. The reboot disconnects the terminal emulator's session with the server.

   If the CD does not eject, you must restart the installation procedures.
7. If the CD ejects correctly, wait three minutes for the reboot to complete.

   You might use **`ping -t`** to alert you when the reboot is complete.
8. When the Avaya Services port is ready again, start up a telnet session, and log in using standard procedures.
9. If prompted to suppress alarm origination, accept the default of **y** for yes, suppress alarms.
10. Run the command **`ifconfig`** at a prompt to verify connectivity of the eth connection of eth 1 and eth 2.

    If connectivity is incorrect, fix it or escalate the problem.

Verify the Avaya server software installation

Perform this procedure on all machines in your configuration. These steps verify that the application can run. Later, you or another person might do a more complete installation check before the customer performs their own customer acceptance testing.

1. After the Avaya Services port is ready again, log in using standard procedures.
2. Use the **`statapp -c`** command to verify that SES services are running.
3. If the processes sipserver and eventserver are not running on your simplex SES host, either check the troubleshooting document for your software, or contact your Avaya representative.
4. If the status of these processes shows **partially up**, wait a few moments and check again. The partially up status indicates a transition.

   The status of all processes should show UP ***except*** the status of sipserver, eventserver and imlogger. The status of sipserver, eventserver and imlogger stay Partially Up and change to UP after the administration is completed.
5. Press **Control C** to quit the statapp command.
6. Set the time and date at the system prompt with the Linux **`date`** command.

Verify firmware on the SAMP module

Perform this portion of the installation on every server in your configuration. Ignore any warnings or errors.

This part of the install checks the firmware version and does the first update of the SAMP module.

Verify the SAMP's firmware after loading the CD.

1. Start a terminal session to the server you are installing, either telnet or ssh, and then type `sampupgrade`.

   If the version of SAMP firmware is up to date, then `sampupgrade` output is as follows:

   ```
   craft@lzccsSamp> sampupgrade
   ==>SAMP FW: AVAYA_CCS_1_0_SP1_BUILD_11 [OK]
   craft@lzccsSamp>
   ```

   If the SAMP firmware is incorrect, the upgrade operation starts automatically. Output is shown below.

   ```
   ==>Update SAMP FW [kernel-0.0109-root-0.0109] to [samp-update-
   AVAYA_CCS_1_0_SP1_BUILD_11.tbz]
   ==>Update SAMP w/ the factory configuration
   ==>Update SAMP for [factory] configuration
   ==>Sync SAMP configuration XML: /usr/hap/etc/avaya109.xml
   ==>Configure eth2(192.11.13.6) device at SAMP
   ==>Wait for the SAMP to reboot with the factory configuration.
   [0]
   ==>Run sampfixer to upgrade SAMP FW now
   Notes:
   SAMP update takes few minutes to complete.
   After firmware upgrade is done, enter "Y" at the
   "Commit [Y|N]" prompt to commit the new firmware.
   The CCS Server will be rebooted at the end.
   ==>Remove /var/home/ftp/pub/samp-update-*.tbz
   ==>Install SAMP FW: /usr/hap/etc/samp-update-
   AVAYA_CCS_1_0_SP1_BUILD_11.tbz
   ==>Synchronize the server's IP address with the SAMP's
   ```

```
==>Update SAMP firmware now
Warning: Permanently added 'my-samp,10.221.248.1' (RSA) to the
list of
known hosts.
1723+1 records in
1723+1 records out
mke2fs 1.27 (8-Mar-2002)
.
.
.
Correct: [y|n] y
The SAMP accepted the new firmware and is rebooting.
```

Run the ccsInstaller script

In this section, run the ccsInstaller once to complete the SAMP upgrade in Verify firmware on the SAMP module on page 93. When complete, run ccsInstaller again to assign names, addresses, and roles to the server.

1. Login and type **`ccsInstaller`** to run the initial configuration script.

   The ccsInstaller script checks the SAMP firmware version and upgrades it if necessary. If the SAMP firmware is running the correct version, ccsInstaller continues. Otherwise, ccsInstaller displays warning messages indicating the current firmware version of SAMP, and then indicating what the correct version should be. The ccsInstaller stops. If ccsInstaller stops with this warning, run the **`sampupgrade`** command to upgrade the SAMP firmware.

   SAMP upgrade takes place automatically, but works the same as in the previous upgrade. This time it will not take as long.

2. When the SAMP upgrade is finished, type **ccsInstaller** again.

- You may want to use the information in Worksheet for Duplication on page 461 to help you answer the prompts in this section.

  After you answer all the questions, ccsInstaller executes several more scripts to update all the files requiring these changes.

  - The ccsInstaller script prompts you for network settings of the SES server:
    - Host name
    - Fully qualified domain name
    - Host IP
    - Network mask
    - Default gateway
    - DNS IP, and so on

3. Select **OK** when you have entered these.
4. Enter the information listed under Setup and configuration on page 61.
5. For the prompt **High Availability configuration option**, answer **y**. This is a duplex installation.
6. Answer these questions:
   - Role of the server to be A, primary or B, backup,
   - The logical host name for the server you are installing
   - The logical IP address used by both servers in the duplex pair
   - The backup server host name, even though it may be off.
   - The backup server physical IP address, even though it may be off

7. For server A only, answer the prompt to abort waiting with **y**.
8. Enter information for initial database setup for the postgreSQL service, such as an mvss password.
9. When prompted with **Are you initializing a Master Administrator on this machine?**, enter **y**.

   Only the edge server in an SES system has a Master Administration interface. You will be prompted with this question only if this is A, the primary server.
10. Choose an mvss database password. This password is required for initial database administration or future troubleshooting.

    You see several status messages regarding the database account, both before and after the following steps.
11. Leave the server A on and repeat this procedure on B, the backup server. Start in again at Load the install CD on page 115 and work to this point.
12. When server A and B are ready, run **`checkconfig`**.
13. Fix any errors, and re-run **`checkconfig`** until no errors remain.
14. Once **`checkconfig`** runs error-free, reboot.

Start SES services on the duplex pair

For both servers, follow these steps:

1. Run the command **checkconfig** on server A to verify the connectivity to the remote server and the network. There should be 9 out of 12 connections reported as SUCCESS. If there are not 9 successful connections, check the configuration completely.
2. Use the **in-service** command on server A first, then on server B second.
3. Use the **reboot** command for both servers.
4. When the A and B servers come up, again enter the **checkconfig** command on both servers. All 12 connections should report SUCCESS.
5. Observe that the **ping** to the virtual IP will fail until all services are started.

Example of the output from the checkconfig command

```
>checkconfig
This is a redundant system Server [ibmx306]
Starting interface checking. This set of tests requres A an B systems
up and running

Info: Checking network connectivity.
        Pinging home3-a eth0 (192.11.14.10): SUCCESS
        Pinging home3-b eth0 (192.11.14.11): SUCCESS
        Pinging home3-a eth2 (192.11.14.31): SUCCESS
        Pinging home3-b eth2 (192.11.14.32): SUCCESS
        Pinging home3-a eth0 (192.11.14.10): SUCCESS
        Pinging Gateway port (172.31.80.1 ): SUCCESS
        Pinging Virtual IP (172.31.80.30): SUCCESS

Info: Checking DNS configuration.
        Pinging Server Virtual IP DNS (home3.mysip.com): SUCCESS
        Pinging home3-a DNS (home3-a.mysip.com): SUCCESS
        Pinging home3-b DNS (home3-b.mysip.com): SUCCESS

Info: Checking remote maintenance board version.
```

```
        Version [AVAYA_CCS_1_0_SP1_BUILD11]

Info: Checking remote maintenance board for home3-a.
        Login to home3-a RSA card is successful.

Info: Checking network configuration for home3-b.
4 Network interfaces found. OK.

Number of tests = 12
Number of passed tests = 12
```

Verify the Avaya server software installation

Perform these steps on server A first and then B:

1. After the Avaya Services port is ready again, log in using standard procedures.
2. Use the **statapp** command on both servers in the duplex pair to verify that SES services are running.
3. If the SipServer and the EventServer processes are not running, either check the troubleshooting document for your software, or contact your Avaya representative.
4. If the status of these processes shows **partially up**, wait a few moments and check again. The partially up status indicates a transition.
5. Server A shows `in-service primary`.
6. Server B shows `in-service backup`.

All processes show the status UP except SIPServer, EventServer, and IMLogger. These three processes show the status of Partially Up until after administration is complete.

Initial administration for home/edge server

The hardware is databased through ART. Once administered, the passwords you set here, and PPP address are provided through ART.

- Select UPDATE on each screen as you work through it.
- The ART script guides you through the steps to administer this information.

Follow these steps:

1. From your browsers, go back and set the laptop to connect to the internet and not act as a dumb terminal to the server.
2. Open a web browser window and type the following in the Address field:

   https://*hostname*/admin

   or

   https://*ipaddress*/admin

   The *hostname* is the fully qualified domain name of the server if you have DNS administered.

   If you do not type **/admin**, the SIP PIM interface for the end user displays.
3. Enter the default administrative user name **admin** in the **Logon ID** field and press Enter.
4. Enter the initial password for the admin account, and select **Logon**.

   Note that after this initial logon, the default password should be changed for security reasons. See Change Administrator Password screen on page 328.

Use the Maintenance interface

At this point, you are logged in through the customer LAN as shown in the connectivity diagrams.

1. From the Administration and Maintenance screen, choose **Maintenance** Interface,
2. Select **Server > Server Date and Time**.

   Set the time and date with the Maintenance page Server Date/Time screen on page 369.
3. Select **Server > Server Configuration > Configure Server**.

   Synchronize the time with an external time source. See Network Time Server screen fields on page 376.
4. Remain in **Server Configuration > Configure Server >** and view all the screens there. Be sure that the fields show the correct data for your site.

5. Select **Security > Authentication File** screen, and make sure all the fields are correct.

   This step is related to the authentication files you downloaded in the pre-installation preparation discussed in Loading the authentication file on page 62.

6. Close that browser and open the page showing Administration and Maintenance interface choices.

Use the Administration interface

At this point, you are still accessing the SES application from the customer LAN connection. In the Administration interface, perform these tasks:

1. Select **Launch Administration Web Interface**.

   You receive a warning about License Error Mode. You may ignore it until after completing the server installation.

2. Select **Setup** to display the first of the Setup screens on page 159.

   Select each link on the **Setup** screen to complete the initial host administration screens.

3. From **Setup**, select **Setup SIP Domain**. The system displays the Edit System Properties screen on page 318. Complete that screen.

   a. Enter the network name or IP address of the SIP domain to which this server is assigned (usually, an enterprise's top level) in the **Domain** field.

   b. In the **License Host** field, enter the physical IP address of server A of the home/edge server on which you intend to enable the WebLM service for this SES system.

   c. Select **Update** and then **Continue**.

4. From **Setup**, select **Setup Hosts**.

   a. On the Add Host screen on page 165, enter the name of the server, for example, edge.customer.com, in the **Host Name** field and select Home/edge from the entries in the drop-down list **Host Type**.

   b. In the **Password** field, enter the mvss database password that you set during installation Step 10 in Run the ccsInstaller script on page 95.

   c. Set up the **Profile Service Password** for the server.

This password provides permissions between the SES hosts, both home server and edge server.

The Profile Service Password is not used by users or administrators. Rather, it is a password that uniquely identifies a proxy for intra- and inter-proxy communication. The Profile Service Password must be unique for each administered host.

d. Set **Listen and Link protocols**.

The only link protocol supported for SIP trunking in Avaya Communication Manager is TLS. By default, the system shows all listen protocols and one link protocol (TLS, for SES host-to-media server communication). You may select your own, so long as any link protocol you select is also selected as a listen protocol.

For example, if you are using a 46xx SIP telephone, or if you are connecting to a SIP service provider, then you could check all three listen protocols. If you are using only the IM client in IP Softphone R5 or SIP Softphone R2 within your enterprise, then the TLS Listen Protocol is sufficient.

e. (Optional) When a SIP client tries to register with this host, by default the minimum-duration registration acceptable is 15 minutes. If you wish to change this value, enter a new, whole integer, 900 through 59,940, in the **Minimum Registration** field.

f. (Optional) You may accept or change the defaults for the following fields:

- Presence Access Policy
- Minimum Registration (seconds)
- Outbound Routing Allowed From
- Outbound Proxy
- Outbound Port
- Outbound Transport
- Outbound Direct Domains

g. Select **Add** and then select **Continue** on the confirmation screen.

h. Select **Update**. All pending updates administered on this host become synchronized on all other hosts.

Note:

REMOVE duplex homes now, then come back to here.....

5. (Optional) Select **Setup Default User Profile** to access the Edit Default User Profile screen on page 172

6. Select **Setup Media Servers** to display the Add Media Server screen on page 174. You must do this step before any media server extensions can be administered.

After these associated screens have been completed, **Setup** disappears from the left-hand menu of choices.

7. Select the Hosts screen, select **Update All** or **Force All** to synchronize the databases the databases.

For details on the use of Update All and Force All, see the appendix Force All and Update All use and behavior on page 471.

8. Change the default password at the top login window for security reasons. See Change Administrator Password screen on page 328.

Server license installation

An SES system requires these licenses:

- Home proxy license
- Edge proxy license
- Home seat licenses

These three licenses are accommodated in one file.

There are three types of licenses. Terminology is different between the Master Admin interface License screen and the WebLM->Licensed Products->IMPRESS screen.

See the table below.

Admin Web Interface	Web LM screen
Edge Proxy	Edge Proxy License (EDGE_proxy)
Basic Proxy	Home Proxy License (BASIC_proxy)
Home Seats	Home Seat Licenses (HOME_seats)

The WebLM server is installed in one location only, on an SES edge server. For a duplexed pair, pick an edge server's physical name or IP address, usually the A server.

Obtain licenses for the Avaya SES system with these steps:

1. To obtain the correct MAC address, go to a command line and type `get-mac-address`.

   Alternatively,

   a. Enable and log in to WebLM using steps 5 through 9 below.

   b. Select **Server Properties**. The contents of the **Primary Host ID** field is the eth0 MAC address of the server.

2. Use your established RFA web procedures for obtaining licenses for Avaya servers.

   a. Use the MAC address you obtained in Step 1.

   b. Go to the RFA web site at http://rfa.avaya.com and download the license file to where you can upload it later on, typically to a location on the PC used by authorized services personnel.

3. You must logon and select the link to the Maintenance Web Interface.
4. From the list of available Security screens, select the link to view the WebLM Software screen.
5. If WebLM is not already enabled, select **Enable WebLM**.

6. From the list of available Security screens, select the link to view the WebLM License Administration screen.
7. Select **Access WebLM**.

   The system displays the WebLM application screen.
8. From the WebLM screen, select **License Administration** and then enter the WebLM default administrative password.
9. After your initial log in, the system prompts you to change the password. WebLM logs you out and expects you to log back in with your new password.
10. Select **Install license**.
11. Then select **Browse** and navigate to the location where you saved the license file in Step 2, and then select Install.

    The proxy server will renew acquired licenses every 5 minutes. However, initially, it has not acquired any licenses (there were none installed) so the proxy server will actually be trying every 60 seconds. Then, once it gets them all, it will renew them every 5 minutes.
12. If you need a server to acquire or re-acquire a license immediately, perhaps to update the number of home server seats you are allowed quickly, use these steps:

    a. Restart an Avaya proxy server manually.

    b. From the Master Administration interface, select the **Services** screen, and then select the proxy server's **Stop** link.

       Confirm that this process has stopped, and select the **Start** link.

Administer Communication Manager and endpoints

At this point you are about three-quarters done. For this portion, get a copy of the document *SIP Support in Avaya Communication Manager*. You will use the administration steps there.

Endpoints for Communication Manager include a variety of devices, terminals or stations:

- Avaya SIP phones
- Third-party SIP phones
- Wireless, digital, and analog endpoints
- Avaya 46xx Softphone
- SIP Softphone R2 or later
- IP Softphone R5 or later
- Before your installation is complete, you must use the established procedures to administer the Communication Manager media server for use with SIP. These steps include adding users of SIP telephones and Avaya SIP Softphones, adding extensions for each user, and updating proxy route patterns, as appropriate.
- A SIP-enabled station, such as the Avaya 46xx, should be administered in Communication Manager 3.0 as an Off-Premises Station (OPS). See the *Avaya Extension to Cellular and OPS Installation and Administration Guide*, Issue 6 or later.

Follow these steps:

1. Administer Communication Manager to work with SIP devices.

   The fields that differ SIP from non-SIP Communication Manager media server setup are detailed in *SIP Support in Avaya Communication Manager*.

   The document includes entries for Signaling Group and Trunk Group setup that are specific to SIP. After you have completed setup in Communication Manager, perform a **Save Translations** to save changes.

2. Set up the telephones and endpoint devices.

   After setting up Avaya SIP Softphone users in Communication Manager as SIP Softphones on (OPTIM/OPS), ensure each client PC has the proper release of Softphone software installed, licensed and configured to use SIP for Instant Messaging (IM). Refer to online help in the SIP Softphone application for more information. You also may wish to verify that these softphones can register with the edge/home, and then can send and receive instant messages, update their contact lists, and so on.

3. Check the endpoint devices

   After administering SIP telephones in Communication Manager, ensure that each telephone has a version of firmware that can support SIP. Note that the Avaya 46xx SIP telephone ***requires*** that you enter a domain name on its SIP Settings page. You may wish to make and receive test calls, too.

For application notes on which third-party SIP endpoints are supported, go to the web site:

`http://www1.avaya.com/enterprise/resourcelibrary/applicationnotes/` and then select the link for **Network Infrastructure** under **DevConnect Product Integration**.

Installing an S8500B simplex edge—duplexed homes

Follow the procedures here to install a single edge server with no backup and a duplexed pair of home servers.

These instructions have you set up the edge server, but drop out before you assign a media servers until the home servers are set up. Drop out and set up home server A, then do home server B. After that, go back and install the media server using the Add Host screen.

Best Practices

- Do not use any form of the Linux `stop -a` or `start -a` commands on a duplexed server. For SES, these commands are disabled.
- Review the information on connections and relate it to your own hardware installation
- Go through all the procedures on the primary server, server A. Then repeat the needed procedures for the backup server, server B.
- Always start installation of duplex systems on the A server.
- When installing the A server, the B server is powered down.
- After installation for the primary server, server A, is completed, leave the A server on.
- Power on the B server and perform the installation on the B server.

Connection schema for the simplex edge server

The connection schema for the duplexed home servers are at Connection schema for the duplex home servers on page 110.

Before beginning the installation procedure, check all connections.

Table 5 shows the port and purpose for an edge simplex configuration.

Important:
If you check the Ethernet port mappings with `ifconfig`, your command output will match the information in the table. If you use a different method, perhaps a web page, your results will differ from what is listed in the table.

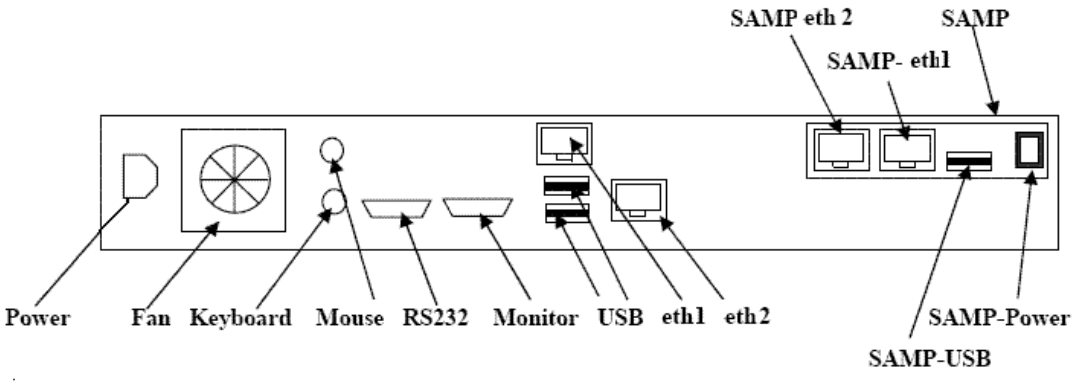
At this point in the installation, the SAMP ethernet ports do not display.

Table 5: S8500B Ethernet Port address assignments

Ethernet Port	Purpose
S8500B motherboard eth1	Connect to customer's LAN
S8500B motherboard eth2	Reserved for Avaya Services
SAMP eth1	Reserved for Avaya Services
SAMP eth2	Unavailable. Connects SAMP to motherboard internally

Figure 8 shows a single S8500 series S8500B port configuration with a single SAMP card installed.

Figure 8: S8500B Port Diagram - simplex



Note:

No additional NIC is required for a simplex configuration.

See Figure 9 for a photograph of the S8500B backplane for your reference.

Figure 9: S8500 series S8500Bwith SAMP card

Follow these steps:

1. Take the S8500B server out of the shipping box and check for damage.
2. Verify that all the required hardware and cabling are present.
3. Ensure that all server components are seated properly.
4. Connect a power cord to the server and the SAMP module.
5. Connect the Services laptop PC to the SAMP.
6. Run the command **`ifconfig`** at a prompt to verify connectivity. If connectivity is incorrect, you will need to escalate the problem.

Connection schema for the duplex home servers

The connection schema for the simplex edge server is at Connection schema for the simplex edge server on page 108.

Before beginning you installation procedure, check all physical connections.

Table 6 shows the port and purpose for an home duplex configuration.

Important:
If you check the Ethernet port mappings with **`ifconfig`**, your command output will match the information in the table. If you use a different method, perhaps a web page, your results will differ from what is listed in the table.

Table 6: S8500B Ethernet Port address assignments

Ethernet Port	Purpose
S8500B eth0	Connect to customer's LAN
S8500B eth3	Reserved for Avaya Services
S8500B eth1 on NIC	Connects Server A:192.11.14.10 to Server B:192.11.14.11
S8500B eth2 on NIC	Not Assigned
S8500B eth4	Unavailable. 192.11.13.1 Connects host and SAMP S8500B
SAMP eth1	Unavailable. 192.11.13.2 Connects SAMP to host internally
SAMP eth2	Connect to other SAMP eth2 with terminator cable.

Figure 10 shows the port numbering for an S8500B duplex configuration, which is different from the numbering on an S8500B simplex configuration.

Figure 10: S8500B Port locations for duplex pair

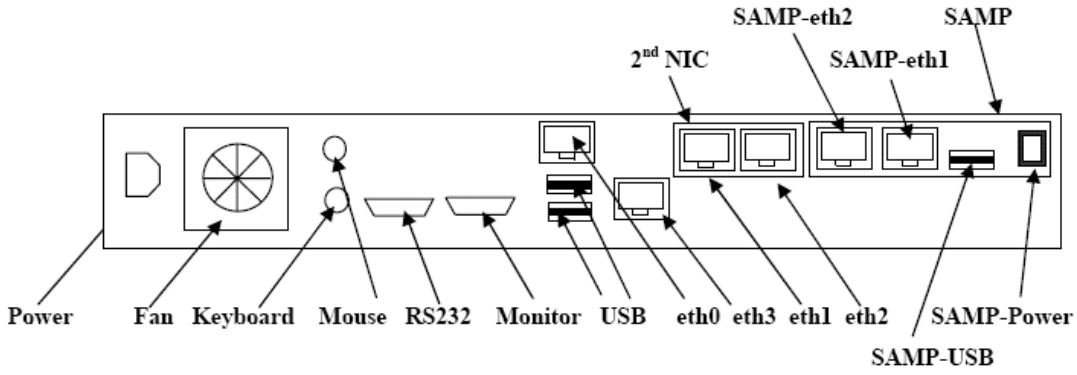
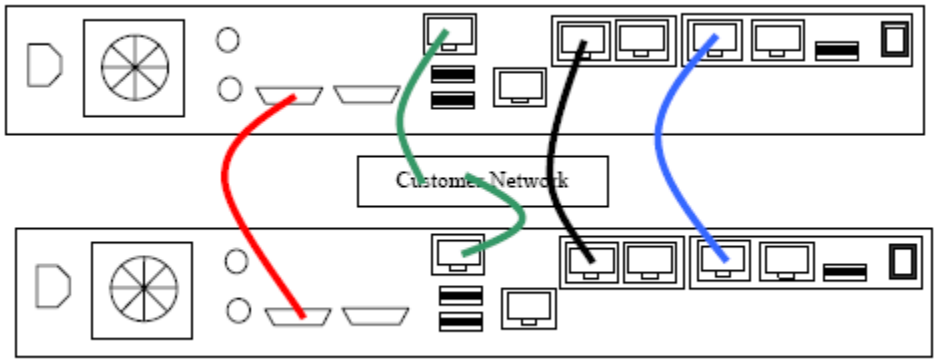


Figure 11 shows how the duplexed pair should be connected.

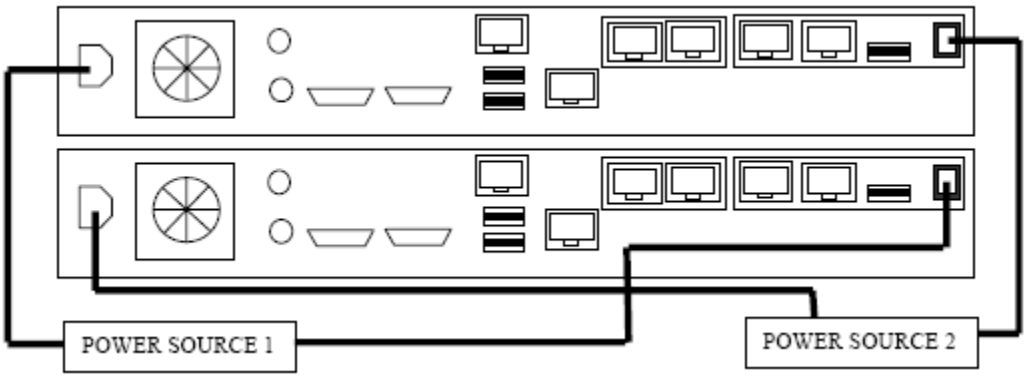
Figure 11: S8500B Duplex connections



- Red - Heartbeat. Null Modem Cable connects both RS232 ports
- Green - Customer Network connection. (S8500B Ethernet port eth0)
- Black - Data Link. Cross-connect LAN cable (S8500B Ethernet port eth1). Connects the motherboards
- Blue - Control Link. Cross-connect LAN cable (SAMP Ethernet port eth2). Connects the SAMP cards.

Figure 12 shows the power connections for the server itself and the SAMP module. Make sure your power cabling is correct.

Figure 12: Power connections for a duplexed pair of S8500B



Disable console redirection

Obtain a keyboard and monitor to connect to the serial port and perform this procedure on only server A.

1. Verify that all the required hardware and cabling are present for all servers.
2. Take the S8500B server out of the shipping box and check for damage.
3. Ensure that all components are seated properly.
4. Connect a power cord, console, and keyboard to the server.
5. Power up the server.
6. The system immediately prompts the BIOS information on console.
7. Press **F1** now.

   You may need to hold down the F1 key to assure that the system displays the BIOS setup page.
8. Select **Advanced Setup**.
9. Select **Console Redirection**.
10. Select **COM port address**.
11. Use the arrow keys to change to **Disabled**.
12. Save changes and exit the BIOS configuration screen.

    The server reboots.

For any other procedures, see:

- Installing and Configuring *the Avaya S8500 Media Server*, Doc ID 03-300143 page 49,
- *Job Aid: Replacing the Dual Network Interface,* Doc ID 555-245-760

Verify firmware and BIOS on the S8500B server

This procedure checks the S8500B server. Perform this procedure on all servers in your configuration.

Perform this procedure on all server.s

The laptop should be on, the server should be off.

1. Connect the laptop PC to eth 3 on the server.

   Alternatively, you may use an RS232 cable to connect to the server.

2. With your browser, make sure that the laptop is not configured to access the internet.

   In MS Internet Explorer for example, click **Control Panel** > **Network Connections** > **Local Area Connections**, and select **TCP/IP**. If necessary, change the IP address so that the laptop performs as a console and does not try to attach to the Internet.

3. From the laptop control panel, open a HyperTerminal session.

   Start > All Programs > Accessories > Communications > Hyperterminal

4. Connect a power cord to the S8500B at this point, not earlier.

5. Power up the S8500B and observe the boot messages in the HyperTerminal window.

   The system immediately prompts for BIOS information.

6. Press F1.

7. Choose **System Summary** and check that the extra RAM has been properly installed and enabled.

   The server should have either 1 gigabyte or 3 gigabytes, depending on the size of the user base. See Hardware requirements on page 36.

8. Choose **Devices** > **IO Ports** > **Primary Master** and verify these BIOS settings:

   a. Verify that the BIOS is set so that the **CD drive** is the first choice of system boot device.

   b. Verify that the server has been upgraded to the minimum Avaya BIOS or an approved later release. There should be BIOS Date and EEPROM fields on the screen. For the S8500B, the minimum version is 21A or greater. To check the BIOS version, follow these steps:

      - Select **System Information** > **Product Data**.
      - There should be BIOS Date and EEPROM fields on the screen.
      - In the EEPROM field, look for a value similar to KEEH**21A**US.

        The notation **21A or 24A** designates the BIOS version. If the BIOS version is earlier than 21A, it is necessary to upgrade the BIOS firmware.

        See *Upgrading firmware on the BIOS—Avaya S8500 Media Server*, document ID 03-300411, for instructions.

Load the install CD

This procedure copies application files to the server and creates file systems.

Perform this procedure on the primary server, A, first and then the backup B server. Keep server B powered off while working with server A. Keep server A on while working on the server B.

Use these steps:

1. Set the IP address of the laptop or PC to 192.11.13.5 and use a netmask of 255.255.255.252.

   You do not need to specify a default gateway.

   Use a CAT 5 cross-connect cable between the ethernet ports of the laptop and the home/edge server.
2. Put the SES R3.0 install CD in the CD drive and close.
3. Turn off the power to the server and cycle the AC power to restart the server by.

   Allow the server to boot from the CD, and wait about 3 minutes.
4. From the laptop, connected to eth 3, start a telnet session to the server you are installing.
   a. In the first window, select this item:
      - **Install or Upgrade CCS Software**
   b. In the second window, select this item:
      - **`Release Version CCS software load number`**

      Wait about 10 minutes for this to complete.
5. Press Enter to accept of each default setting.

   Accept these defaults to install the new release on this server.
6. Type **y** or Enter to proceed.

   The server copies the software Redhat package managers to the appropriate partition.

   The server ejects the CD from the drive and reboots. The reboot disconnects the terminal emulator's session with the server.

   If the CD does not eject, you must restart the installation procedures.
7. If the CD ejects correctly, wait three minutes for the reboot to complete.

   You might use **`ping -t`** to alert you when the reboot is complete.
8. When the Avaya Services port is ready again, start up a telnet session, and log in using standard procedures.
9. If prompted to suppress alarm origination, accept the default of **y** for yes, suppress alarms.
10. Run the command **`ifconfig`** at a prompt to verify connectivity of the eth connection of eth 1 and eth 2.

    If connectivity is incorrect, fix it or escalate the problem.

Verify the Avaya server software installation

Perform this procedure on all machines in your configuration. These steps verify that the SES application can run. Later, you or another person might do a more complete installation check before the customer performs their own customer acceptance testing.

1. After the Avaya Services port is ready again, log in using standard procedures.
2. Use the **`statapp -c`** command to verify that SES services are running
3. If the processes sipserver and eventserver are not running on your simplex SES host, either check the troubleshooting document for your software, or contact your Avaya representative.
4. If the status of these processes shows **partially up**, wait a few moments and check again. The partially up status indicates a transition.

   The status of all processes should show UP ***except*** the status of sipserver, eventserver and imlogger. The status of sipserver, eventserver and imlogger stay Partially Up and change to UP after SES server administration is completed.
5. Press **Control C** to quit the statapp command.
6. Set the time and date at the system prompt with the Linux **`date`** command.

Verify the firmware on the SAMP

Perform this portion of the installation on every server in your configuration. Ignore any warnings or errors.

This part of the install checks and does the first update of the SAMP module.

Verify the SAMP's firmware after loading the CD.

1. Start a terminal session to the server you are installing, either telnet or ssh, and then type `sampupgrade`.

   If the version of SAMP firmware is up to date, then `sampupgrade` output is as follows:

   ```
   craft@lzccsSamp> sampupgrade
   ==>SAMP FW: AVAYA_CCS_1_0_SP1_BUILD_11 [OK]
   craft@lzccsSamp>
   ```

   If the SAMP firmware is incorrect, the upgrade operation starts automatically. Output is shown below.

   ```
   ==>Update SAMP FW [kernel-0.0109-root-0.0109] to [samp-update-
   AVAYA_CCS_1_0_SP1_BUILD_11.tbz]
   ==>Update SAMP w/ the factory configuration
   ==>Update SAMP for [factory] configuration
   ==>Sync SAMP configuration XML: /usr/hap/etc/avaya109.xml
   ==>Configure eth2(192.11.13.6) device at SAMP
   ==>Wait for the SAMP to reboot with the factory configuration.
   [0]
   ==>Run sampfixer to upgrade SAMP FW now
   Notes:
   SAMP update takes few minutes to complete.
   After firmware upgrade is done, enter "Y" at the
   "Commit [Y|N]" prompt to commit the new firmware.
   The CCS Server will be rebooted at the end.
   ==>Remove /var/home/ftp/pub/samp-update-*.tbz
   ==>Install SAMP FW: /usr/hap/etc/samp-update-
   AVAYA_CCS_1_0_SP1_BUILD_11.tbz
   ==>Synchronize the server's IP address with the SAMP's
   ==>Update SAMP firmware now
   ```

```
Warning: Permanently added 'my-samp,10.221.248.1' (RSA) to the
list of

known hosts.

1723+1 records in

1723+1 records out

mke2fs 1.27 (8-Mar-2002)

.

.

.

Correct: [y|n] y

The SAMP accepted the new firmware and is rebooting.
```

Run the ccsInstaller script for the edge server

In this section, run the ccsInstaller once to complete the SAMP upgrade you started in Verify the firmware on the SAMP on page 117. When complete, run ccsInstaller again to assign names, addresses, and roles to the server.

1. Login and type **`ccsInstaller`** to run the initial configuration script for the SES host machines.

   The ccsInstaller script checks the SAMP firmware version and upgrades it if necessary. If the SAMP firmware is running the correct version, ccsInstaller continues. Otherwise, ccsInstaller displays warning messages indicating the current firmware version of SAMP, and then indicating what the correct version should be. The ccsInstaller stops. If ccsInstaller stops with this warning, run the `sampupgrade` command to upgrade the SAMP firmware.

   SAMP upgrade takes place automatically, but works the same as in the previous upgrade. This time it will not take as long.

2. When the SAMP upgrade is finished, type **ccsInstaller** again.

- You may want to use the information in Worksheet for Duplication on page 461 to help you answer the prompts in this section.

  After you answer all the questions, ccsInstaller executes several more scripts to update all the files requiring these changes.

  - The ccsInstaller script prompts you for network settings of the SES server:
    - Host name
    - Fully qualified domain name
    - Host IP
    - Network mask
    - Default gateway
    - DNS IP, and so on

3. Select **OK** after you have entered these.
4. Enter the information listed under Chapter 6: Setup and configuration on page 61.
5. For the prompt **High Availability configuration option**: answer **n**. This is a simplex edge installation.
6. Enter information for initial database setup for the postgreSQL service, such as an mvss password.

7. Choose an mvss database password. This password is required for initial database administration or future troubleshooting.

   Note the several status messages regarding the database account, both before and after the following steps. After those messages, web services restarts.

8. For the prompt **Are you initializing a Master Administrator on this machine**, enter **y**.
9. For the prompt **Start Services**, answer **y.**

Run the ccsInstaller script for the home servers

In this section, run the ccsInstaller once to complete the SAMP upgrade in Verify the firmware on the SAMP on page 117. When complete, run ccsInstaller again to assign names, addresses, and roles to the server.

1. Login and type **`ccsInstaller`** to run the initial configuration script.

   The ccsInstaller script checks the SAMP firmware version and upgrades it if necessary. If the SAMP firmware is running the correct version, ccsInstaller continues. Otherwise, ccsInstaller displays warning messages indicating the current firmware version of SAMP, and then indicating what the correct version should be. The ccsInstaller stops. If ccsInstaller stops with this warning, run the **`sampupgrade`** command to upgrade the SAMP firmware.

   SAMP upgrade takes place automatically, but works the same as in the previous upgrade. This time it will not take as long.

2. When the SAMP upgrade is finished, type **ccsInstaller** again.

- You may want to use the information in Worksheet for Duplication on page 461 to help you answer the prompts in this section.

  After you answer all the questions, ccsInstaller executes several more scripts to update all the files requiring these changes.

  - The ccsInstaller script prompts you for network settings of the SES server:
    - Host name
    - Fully qualified domain name
    - Host IP
    - Network mask
    - Default gateway
    - DNS IP, and so on

3. Select **OK** when you have entered these.
4. Enter the information listed under Chapter 6: Setup and configuration on page 61.
5. For the prompt **High Availability configuration option**, answer **y**. This is a duplex home installation.

6. Answer these questions:
   - Role of the server to be A, primary or B, backup,
   - The logical host name for the server you are installing
   - The logical IP address used by both servers in the duplex pair
   - The backup server host name, even though it may be off.
   - The backup server physical IP address, even though it may be off
7. For server A only, answer the prompt to abort waiting with **y**.
8. Enter information for initial database setup for the postgreSQL service, such as an mvss password.
9. When prompted with “Are you initializing a Master Administrator on this machine?”, enter **n**.

   You did this for the edge server. Only the edge server in an SES system has a Master Administration interface.
10. Choose an mvss database password. This password is required for initial database administration or future troubleshooting.

    You see several status messages regarding the database account, both before and after the following steps.
11. Leave the primary server on and repeat this procedure on the B, backup server. Start in again at Load the install CD on page 115 and work to this point.
12. When server A and B are ready, run **`checkconfig`**.
13. Fix any errors, and re-run **`checkconfig`** until no errors remain.
14. Once **`checkconfig`** runs error-free, reboot.

Verify the software installation

Perform this procedure on all machines in your configuration. These steps verify that the SES application can run. Later, you or another person might do a more complete installation check before the customer performs their own customer acceptance testing.

1. After the Avaya Services port is ready again, log in using standard procedures.
2. Use the **`statapp -c`** command to verify that SES services are running.
3. If the processes sipserver and eventserver are not running on your simplex SES host, either check the troubleshooting document for your software, or contact your Avaya representative.
4. If the status of these processes shows **partially up**, wait a few moments and check again. The partially up status indicates a transition.

   The status of all processes should show UP ***except*** the status of sipserver, eventserver and imlogger. The status of sipserver, eventserver and imlogger stay Partially Up and change to UP after the SES server administration is completed.
5. Press **Control C** to quit the statapp command.
6. Set the time and date at the system prompt with the Linux **`date`** command.

Initial administration

The hardware is databased through ART. Once administered, the passwords you set here, and PPP address are provided through ART.

- Select UPDATE on each screen as you work through it.
- The ART script guides you through the steps to administer this information.

Follow these steps:

1. From your browsers, go back and set the laptop to connect to the internet and not act as a dumb terminal to the server.
2. Open a web browser window and type the following in the Address field:

   https://*hostname*/admin

   or

   https://*ipaddress*/admin

   The *hostname* is the fully qualified domain name of the server if you have DNS administered.

   If you do not type **/admin**, the SIP PIM interface for the end user displays.
3. Enter the default administrative user name **admin** in the **Logon ID** field and press Enter.
4. Enter the initial password for the admin account, and select **Logon**.

   Note that after this initial logon, the default password should be changed for security reasons. See Change Administrator Password screen on page 328.

Use the Maintenance interface

At this point, you are logged in through the cosmetic LAN as shown in the connectivity diagrams.

In the Maintenance interface, perform these tasks:

1. From the log in screen, choose **Maintenance** Interface,
2. Select **Server > Server Date and Time**.

   Set the time and date with the Maintenance page Server Date/Time screen on page 369.
3. Select **Server > Server Configuration > Configure Server**.

   Synchronize the time with an external time source. See Network Time Server screen fields on page 376.
4. Select **Server Configuration > Configure Server >** and view all the screens there. Be sure that the fields show the correct data for your site.

5. Remain in the **Security > Authentication File** screens and make sure all the fields are correct.

   This step is related to the authentication files you downloaded in the pre-installation preparation discussed in Loading the authentication file on page 62.

6. Close that browser and open the main page showing Administration and Maintenance interface choices.

Use the Administration interface

At this point, you are still accessing the SES servers from the customer LAN connection. In the Administration interface, perform these tasks:

1. Select **Launch Administration Web Interface**.

   You receive a warning about License Error Mode. You may ignore it until after completing the server installation.

2. Select **Setup** to display the first of the Setup screens on page 159.

   Select each link on the **Setup** screen to complete the initial host administration screens.

3. From **Setup**, select **Setup SIP Domain**. The system displays the Edit System Properties screen on page 318. Complete that screen.

   a. Enter the network name or IP address of the SIP domain to which this server is assigned (usually, an enterprise's top level) in the **Domain** field.

   b. In the **License Host** field, enter the physical IP address of the edge server.

   c. Select **Update** and then **Continue**.

4. From **Setup**, select **Setup Hosts**.

   a. On the Add Host screen on page 165, enter the name of the server, for example, edge.customer.com, in the **Host Name** field and select Home or Edge from the entries in the drop-down list **Host Type**.

   b. In the **Password** field, enter the mvss database password that you set during installation Step 10 in Run the ccsInstaller script for the home servers on page 121.

   c. Set up the **Profile Service Password** for the server.

      This password provides permissions between the SES hosts, both home server and edge server.

      The Profile Service Password is not used by users or administrators. Rather, it is a password that uniquely identifies a proxy for intra- and inter-proxy communication. The Profile Service Password must be unique for each administered host.

d. Set **Listen and Link protocols**.

   The only link protocol supported for SIP trunking in Avaya Communication Manager is TLS. By default, the system shows all listen protocols and one link protocol (TLS, for SES host-to-media server communication). You may select your own, so long as any link protocol you select is also selected as a listen protocol.

   For example, if you are using a 46xx SIP telephone, or if you are connecting to a SIP service provider, then you could check all three listen protocols. If you are using only the IM client in IP Softphone R5 or SIP Softphone R2 within your enterprise, then the TLS Listen Protocol is sufficient.

e. (Optional) When a SIP client tries to register with this host, by default the minimum-duration registration acceptable is 15 minutes. If you wish to change this value, enter a new, whole integer, 900 through 59,940, in the **Minimum Registration** field.

f. (Optional) You may accept or change the defaults for the following fields:

   - Presence Access Policy
   - Minimum Registration (seconds)
   - Outbound Routing Allowed From
   - Outbound Proxy
   - Outbound Port
   - Outbound Transport
   - Outbound Direct Domains

g. Select **Add** and then select **Continue** on the confirmation screen.

h. Select **Update**. All pending updates administered on this host become synchronized on all other hosts.

5. Stop and begin again on the other home server at Load the install CD on page 115. then proceed with the next steps.
6. (Optional) Select **Setup Default User Profile** to access the Edit Default User Profile screen on page 172.
7. Select **Setup Media Servers** to display the Add Media Server screen on page 174. You must do this step before any media server extensions can be administered.

   After these associated screens have been completed, **Setup** disappears from the left-hand menu of choices.
8. Select the Hosts screen, select **Update All** or **Force All** to synchronize the databases the databases.

   For details on the use of Update All and Force All, see the appendix Force All and Update All use and behavior on page 471.
9. Change the default password at the top login window for security reasons. See Change Administrator Password screen on page 328.

Start services on the duplex pair

For both home servers, follow these steps:

1. Run the command **checkconfig** on server A to verify the connectivity to the remote server and the network. There should be 9 out of 12 connections reported as SUCCESS. If there are not 9 successful connections, check the configuration completely.
2. Type the **in-service** command on server A first, then on server B second.
3. Type the **reboot** command for both servers.
4. When the A and B servers come up, again enter the **checkconfig** command on both servers. All 12 connections should report SUCCESS.
5. Observe that the **ping** to the virtual IP will fail until all services are started.

Example of the output from the checkconfig command

```
>checkconfig
This is a redundant system Server [ibmx306]
Starting interface checking. This set of tests requres A an B systems
up and running


Info: Checking network connectivity.
        Pinging home3-a eth0 (192.11.14.10): SUCCESS
        Pinging home3-b eth0 (192.11.14.11): SUCCESS
        Pinging home3-a eth2 (192.11.14.31): SUCCESS
        Pinging home3-b eth2 (192.11.14.32): SUCCESS
        Pinging home3-a eth0 (192.11.14.10): SUCCESS
        Pinging Gateway port (172.31.80.1 ): SUCCESS
        Pinging Virtual IP (172.31.80.30): SUCCESS


Info: Checking DNS configuration.
        Pinging Server Virtual IP DNS (home3.mysip.com): SUCCESS
        Pinging home3-a DNS (home3-a.mysip.com): SUCCESS
        Pinging home3-b DNS (home3-b.mysip.com): SUCCESS
```

```
Info: Checking remote maintenance board version.
        Version [AVAYA_CCS_1_0_SP1_BUILD11]

Info: Checking remote maintenance board for home3-a.
        Login to home3-a RSA card is successful.

Info: Checking network configuration for home3-b.
4 Network interfaces found. OK.

Number of tests = 12
Number of passed tests = 12
```

Server licence installation

An SES system requires these licenses:

- Home proxy license
- Edge proxy license
- Home seat licenses

These three licenses are accommodated in one file.

There are three types of licenses. Terminology is different between the Master Admin interface License screen and the WebLM->Licensed Products->IMPRESS screen.

See the table below.

Admin Web Interface	Web LM screen
Edge Proxy	Edge Proxy License (EDGE_proxy)
Basic Proxy	Home Proxy License (BASIC_proxy)
Home Seats	Home Seat Licenses (HOME_seats)

The WebLM server is installed in one location only, on an SES edge server. For a duplexed pair, pick an edge server's physical name or IP address, usually the A server.

Obtain licenses for the Avaya SES system with these steps:

1. To obtain the correct MAC address, go to a command line and type `get-mac-address`.

   Alternatively,

   a. Enable and log in to WebLM using steps 5 through 9 below.

   b. Select **Server Properties**. The contents of the **Primary Host ID** field is the eth0 MAC address of the server.

2. Use your established RFA web procedures for obtaining licenses for Avaya servers.

   a. Use the MAC address you obtained in Step 1.

   b. Go to the RFA web site at http://rfa.avaya.com and download the license file to where you can upload it later on, typically to a location on the PC used by authorized services personnel.

3. You must logon and select the link to the Maintenance Web Interface.
4. From the list of available Security screens, select the link to view the WebLM Software screen.
5. If WebLM is not already enabled, select **Enable WebLM**.

6. From the list of available Security screens, select the link to view the WebLM License Administration screen.
7. Select **Access WebLM**.

   The system displays the WebLM application screen.
8. From the WebLM screen, select **License Administration** and then enter the WebLM default administrative password.
9. After your initial log in, the system prompts you to change the password. WebLM logs you out and expects you to log back in with your new password.
10. Select **Install license**.
11. Then select **Browse** and navigate to the location where you saved the license file in Step 2, and then select Install.

    The proxy server will renew acquired licenses every 5 minutes. However, initially, it has not acquired any licenses (there were none installed) so the proxy server will actually be trying every 60 seconds. Then, once it gets them all, it will renew them every 5 minutes.
12. If you need a server to acquire or re-acquire a license immediately, perhaps to update the number of home server seats you are allowed quickly, use these steps:

    a. Restart an Avaya proxy server manually.

    b. From the Master Administration interface, select the **Services** screen, and then select the proxy server's **Stop** link.

       Confirm that this process has stopped, and select the **Start** link.

Administer Communication Manager and endpoints

At this point you are about three-quarters done. For this portion, get a copy of the document *SIP Support in Avaya Communication Manager*. You will use the administration steps there.

Endpoints for Communication Manager include a variety of devices, terminals or stations:

- Avaya SIP phones
- Third-party SIP phones
- Wireless, digital, and analog endpoints
- Avaya 46xx Softphone
- SIP Softphone R2 or later
- IP Softphone R5 or later
- Before your installation is complete, you must use the established procedures to administer the Communication Manager media server for use with SIP. These steps include adding users of SIP telephones and Avaya SIP Softphones, adding extensions for each user, and updating proxy route patterns, as appropriate.
- A SIP-enabled station, such as the Avaya 46xx, should be administered in Communication Manager 3.0 as an Off-Premises Station (OPS). See the *Avaya Extension to Cellular and OPS Installation and Administration Guide*, Issue 6 or later.

Follow these steps:

1. Administer Communication Manager to work with SIP devices.

   The fields that differ SIP from non-SIP Communication Manager media server setup are detailed in *SIP Support in Avaya Communication Manager*.

   The document includes entries for Signaling Group and Trunk Group setup that are specific to SIP. After you have completed setup in Communication Manager, perform a **Save Translations** to save changes.

2. Set up the telephones and endpoint devices.

   After setting up Avaya SIP Softphone users in Communication Manager as SIP Softphones on (OPTIM/OPS), ensure each client PC has the proper release of Softphone software installed, licensed and configured to use SIP for Instant Messaging (IM). Refer to online help in the SIP Softphone application for more information. You also may wish to verify that these softphones can register with the edge/home, and then can send and receive instant messages, update their contact lists, and so on.

3. Check the endpoint devices

   After administering SIP telephones in Communication Manager, ensure that each telephone has a version of firmware that can support SIP. Note that the Avaya 46xx SIP telephone ***requires*** that you enter a domain name on its SIP Settings page. You may wish to make and receive test calls, too.

For application notes on which third-party SIP endpoints are supported, go to the web site:

`http://www1.avaya.com/enterprise/resourcelibrary/applicationnotes/` and then select the link for **Network Infrastructure** under **DevConnect Product Integration**.

Installing SES R3.0 on an S8500 server

This section provides installation instructions for installing SES R3.0 on an S8500 hardware base.

- Installing an S8500 distributed edge—duplex with distributed homes—duplex on page 133

Installing an S8500 distributed edge—duplex with distributed homes—duplex

The installation tasks must be performed locally.

Best Practices

- Always start installation of duplex systems on server A.
- When installing the primary server, the backup server is powered down.
- After installation of the primary server is completed, leave the primary server on.
- Power on the backup server and perform the installation on the backup server.
- Do not use any form of the Linux `stop -a` or `start -a` commands on a duplexed server. Doing so may stop all process.
- Review the information on connections and relate it to your own hardware installation.

Connection schema

Before beginning you installation procedure, make all physical connections.

Table 7 shows the port and purpose for an home/edge duplex configuration.

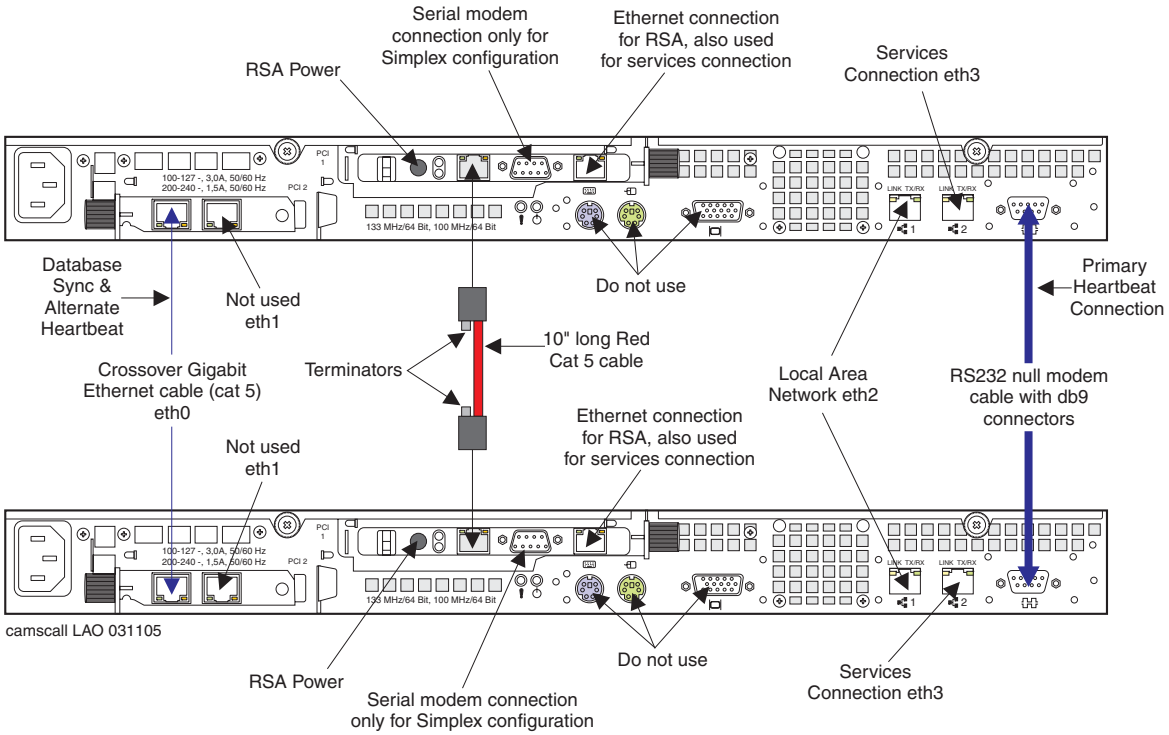
Important:
If you check the Ethernet port mappings with **`ifconfig`**, your command output will match the information in the table. If you use a different method, perhaps a web page, your results will differ from what is listed in the table.

Table 7: S8500 Ethernet Port address assignments

Ethernet Port	IP Address
S8500 eth0	Connect Server A: 192.11.14.10 to Server B: 192.11.14.11 for database synchronization and alternate heartbeat
S8500 eth1	Not Assigned
S8500 eth2	Customer LAN
S8500 eth3	Services
S8500 RS232	Connect server A to server B for primary heartbeat service
RSA RJ 45 eth1	Reserved for services
RSA RJ 11 eth2	Connect RSA A to RSA B

Figure 13 shows the eth port numbering and the connections between an S8500 duplexed pair.

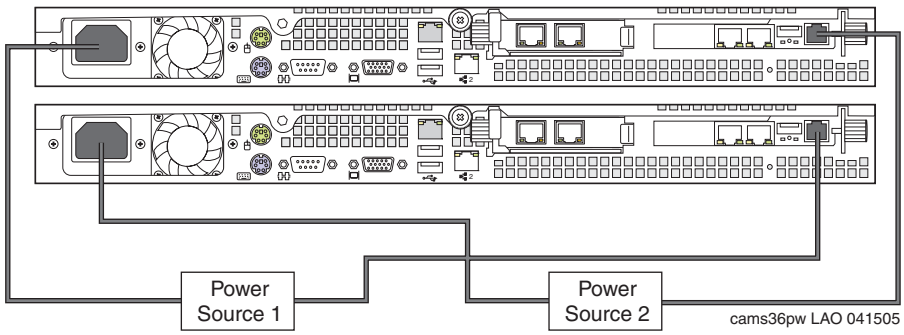
Figure 13: Port locations and connections for S8500 duplex



Eth3 on both servers is reserved for Services.

Figure 14 shows the power connections for the server itself and the SAMP module. Make sure your power cabling is correct.

Figure 14: Power connections for a duplexed pair of S8500



Disable console redirection

On the S8500 redirection of output is disabled and you must enable it.

Obtain a keyboard and monitor to connect to the serial port and perform this procedure on only server A.

1. Verify that all the required hardware and cabling are present for all servers.
2. Attach a keyboard and monitor to the back of the server.

   Take the S8500 server out of the shipping box and check for damage.
3. Ensure that all components are seated properly.
4. Connect a power cord, console, and keyboard to the server.
5. Power up the server.
6. The system immediately prompts the BIOS information on console.
7. Press F1 now.

   You may have a short-timing window here.

   You may need to hold down the F1 key to assure that the system displays the BIOS setup page.
8. Select **Advanced Setup**.
9. Select **Console Redirection**.
10. Select **COM port address**.
11. Use the arrow keys to change to **Disabled**.
12. Save changes and exit the BIOS configuration screen.

The server reboots.

For any other procedures, see:

- *Installing and Configuring the Avaya S8500 Media Server*, Doc ID 03-300143 page 49,
- *Job Aid: Replacing the Dual Network Interface,* Doc ID 555-245-760

Verify firmware on the RSA module

Follow these steps:

1. Verify that all the required hardware and cabling connections are present for all servers
2. There should be two RSA cards in each of the servers in the duplexed pair. Check both of them.
3. Each card must connect to a power source different from the server's power cord.
   The firmware on the RSA should be present and the module seated firmly.
4. Attach a keyboard and monitor to the serial port on the RSA card.
5. Connect a laptop to the RSA's RJ11 jack, log in to the RSA and disable the watchdog timer.
6. Check the firmware on the RSA module.

   The firmware version on the card should be PLET08A, PLEH08B, or PLBH08B.

   See Step a in Run the ccsInstaller script on page 141 for more details on this topic.

   For procedures on verifying and updating the RSA firmware, refer to the documents listed on Related resources on page 20.

Disable the RSA loader watchdog

These steps disable RSA loader watchdog.

1. Log on as **craft**, using the initial craft or unique customer password.
2. Under **ASM Control** click **System Settings**.
3. In the Loader watchdog field, click **Disabled**.
4. Click **Save**.

Log off the RSA

These steps log you off the RSA.

1. From the left pane, select **Log Off**.
2. In the confirmation window, select **Yes**.

Verify the hardware and BIOS on the servers

The BIOS version should be 68A for the series S8500.

- Be sure that the additional, dual NIC has been installed.

  For detailed procedures, refer to:

  - *Installing and Configuring the Avaya S8500 Media Server*, Doc ID 03-300143 page 49.
  - *Job Aid: Replacing the Dual Network Interface,* Doc ID 555-245-760

  CAUTION:

  Make sure that any components like the dual NIC and RSA module are properly seated before continuing. For example, if the dual NIC is *not* properly installed in its slot, an amber LED on the front panel of the server indicates the hardware alarms associated with it.

Perform this procedure on both server A and the server B.

1. From the laptop, open a HyperTerminal session.
2. Connect a power cord to the S8500 at this point.
3. Power up the S8500 and observe the boot messages in the HyperTerminal window.
4. The system immediately prompts for BIOS information.
5. Press F1.

   Check that the extra RAM has been properly installed and enabled in the BIOS.

   The server should have either 1 gigabyte or 3 gigabytes, depending on the size of the user base. See Hardware requirements on page 36.

6. Verify these BIOS settings:

   - Verify that the BIOS is set so that the CD drive is the first choice of system boot device.
   - Verify that the server has been upgraded to the minimum Avaya BIOS or an approved later release. There should be BIOS Date and EEPROM fields on the screen. See Upgrading firmware on the BIOS—Avaya S8500 Media Server, *document ID 03-300411, for instructions.*

Best Practices

For the next two sections, this list shows you, in general, the order in which to load, install, and bring a duplex pair into service.

- At step v, do not start services on the A server,
- Load and install server B.
- Configure both server A and B using the Master Administration interface.
- in service A
- in service B
- Reboot A
- Reboot B

Load the CD

These steps load the needed files onto the hard drive of the server.

1. Put the SES R3.0 install CD in the CD drive and close.
2. Turn off the power to the server.
3. Restart the server by cycling AC power.

   Allow the server to boot from the CD. When Linux loads into RAM[1], the Avaya Services port will be ready in about 3 minutes.

   The system displays a task list (**`Install or Upgrade CCS Software`**) and the **`Release Version`** (the SES software load number).
4. Press ENTER to acknowledge selection of each (default) setting.

   Acceptance of these defaults permits the installing of a new release of SES on this server.
5. Type **y** to proceed.

   After selections are complete, the software RPMs are copied to the appropriate partition.

   The CD is ejected from the drive and the server reboots from the hard-disk drive. The reboot disconnects the terminal emulator's session with the server.

   If the CD does not eject, you must restart the installation procedures.
6. Wait three minutes for the reboot to come up.

1 This may also be referred to as NV RAM.

Run the ccsInstaller script

Use these steps to work through the install script questions.

1. Check and upgrade the firmware of the RSA if necessary.
   a. Type `cd /opt/IBMmpcli/bin`
   b. Type `./mpcli`
   c. Type `logonlocal`
   d. After the SUCCESS message, type `getvpd -mprom`
   e. If you have the required firmware, the build ID on both servers of a duplex pair should be one of the following:
      - PLEH*08A*
      - PLEH*08B*
      - PLBH08B

      In the example above, the last three characters vary with the version number.

      In the example above, if you see T instead of H, you must update the firmware.

      If the build ID is different, refer to Avaya's Support web site and the documents for details on upgrading to the latest firmware.
   f. Type `logoff`
   g. After the SUCCESS message, type `exit`

      You are returned to the root user login prompt.
2. Login and type **`ccsInstaller`** to run the initial configuration script.

   You may want to use the information in Appendix B: Worksheet for Duplication on page 461 to help you answer the prompts in this section.
3. The ccsInstaller script prompts you for the following information:
   a. Network settings of the SES server (select OK when you have entered these).
   b. Network settings for the ethernet port of the RSA module in this server.
   c. For the High Availability configuration option, type y. High Availability means you have a duplexed pair.
   d. When asked My Role in the Redundant Infrastructure?, that is, is this server's role active or standby, select A if you are installing the active server or select B if you are installing the backup server.
   e. Enter the logical name referring to the duplex server pair.
   f. Enter the logical static IP address referring to the duplex server pair.

g. Enter the physical host name and IP address of the other server in this duplex pair (that is, the name of the standby server if you are installing active server, or the name of the active server if you are installing standby server).

h. Enter the user name and password for an administrative login of the RSA module on the active server of the pair.

i. For an RSA module with the latest Avaya firmware, you may use the RSA user name of **craft** and a valid password. Note that this RSA user login information may have changed when the module was installed or upon a full reset.

j. Enter the host name and IP address of the RSA module on the standby server.

k. Enter user name and password for an administrative login of the RSA module on the standby server.

l. If this is the first of the two servers you have configured, the system message asks *Do you want to abort waiting for other server and make this one primary?*

m. Do not answer, just stand by and wait for the question to time out. The system displays several informational messages, followed by **Waiting for Sync to finish...**: This process takes 5 to 10 minutes to completely synchronize the primary and backup servers. Answering with any response creates a rolling reboot trouble.

n. After several warning messages that the other server is not responding, a default interval for waiting expires, and the ccsInstaller script continues.

o. Note the several messages regarding duplex services (drbd, Heartbeat), each with OK.

p. After viewing those messages, continue with initializing the database setup.

q. Enter information for initial database setup (for the postgreSQL service), such as an mvss password.

r. Choose an mvss database password. This password will be required for initial database administration for future troubleshooting.

   You should see several status messages regarding the database account, both before and after the following steps. After those messages, web services restarts.

   This step is skipped on the first server of the duplex pair, but available for the standby server B.

s. Enter y to install a Master Administrator interface on the server you are installing. Enter n to install a Limited Administrator interface.

   Only edge servers have the Master Administration interface. Home servers have a Limited Administrator interface. The Master Administration interface can add and delete users, and update data on all home or edge servers in a domain. The Limited Administrator interface cannot update user data but provides all other functions.

   The system asks if you wish to install a Master Administrator interface on this server only if you have *not* specified previously that a server will have the Master Administrator interface.

t. Enter the IP address of the S8500 server that has the Master Administration interface, but only if you answered **no** to installing a Master Administration interface in the preceding step.

   On duplex servers, this is a logical IP address for the pair. When configuring a home server, which has no Master Administrator interface, enter the IP address of the edge server that is running the Master Administrator interface in your SES system.

   For example, enter the IP address of the edge that controls this home server.

u. Enter the password for the heartbeat service to use (must be the same password on both the active and standby servers).

   This password may be required for troubleshooting duplex server configurations.

v. Indicate whether you want to start services now.

   For either server A or B of a duplex server pair, always answer **n**.

   You will start services later.

Install Server B

Do the following for the other server:

1. Repeat the preceding procedure Load the CD on page 140
2. Repeat the procedure, Run the ccsInstaller script on page 141 to configure the standby B server.
3. After configuring B, do not start services on the B server either.
4. At this point, both of the duplex servers, A and B, are out-of-service.

Verify the software installation

After the Avaya Services port is ready again, log in using standard procedures.

1. At the root user login prompt, run the command **`checkconfig`** on either server in the duplex pair to test proper connectivity to the network, and to the other duplex server.

   The output of this command should report several SUCCESS messages, and ultimately the total number of tests that were run and passed. If any tests fail unexpectedly, verify and repair the condition, as needed.

   You may expect that the tests checking the DNS configuration will fail if DNS has not been configured on your network.

   When working on the backup server of a duplexed pair, also expect this test to fail: **Pinging Virtual IP**. At this point there is no primary server running.

2. Enter `in-service` at the root prompt on the B server to put server B into service.
3. Enter `server` to verify the B server's status is in service.

   When working on the backup server in a duplexed pair, the status shows **Not Ready (In Service--heartbeat not running.** This is the correct status for the backup at this point.

4. Repeat Steps 1 through 3 for the A server in the duplex pair.
5. Enter `reboot` on the A server to reboot server A.
6. Wait about five minutes for the software to initialize on this server, ignoring any questions or messages you receive until this interval is over.

   While waiting, you can run the **`statapp`** command to view the status of SES-related applications. After initialization is complete on this server, the results of the command should report UP.

7. Enter **`server`** to confirm that server A is active.
8. Reboot server B by performing Steps 1 through 7 on the B server.

   Both servers should now report they are active and in service. One of the two servers should be Primary and the other server should be the Backup.

   Test these server modes by executing the **`takeover`** command on the backup server to make it the primary.

9. Before beginning the next phase of installation, re-enable the RSA loader watchdog.

Start services on the duplex pair

To start services on the duplex pair, follow these steps:

1. After installation to this point is complete on both A and B servers, run the command **checkconfig** on both servers to verify the connectivity to the remote server and the network. There should be 9 out of 12 connections reported as SUCCESS. If there are not 9 successful connections, check the configuration completely.
2. Run the **in-service** command for both servers.
3. Run the **reboot** command for both servers.
4. When the A and B servers come up, perform the **checkconfig** command on both servers. All 12 connections should report SUCCESS.

Example of the output from the checkconfig command

When the SES-related services start successfully, you should see a series of OK messages.

```
> checkconfig

This is a redundant system. Server [ibmx305]

Starting interface checking. This set of tests requires A and B systems
up and running


Info: Checking network connectivity.
        Pinging home3-a eth0  (192.11.14.10): SUCCESS
        Pinging home3-b eth0  (192.11.14.11): SUCCESS
        Pinging home3-a eth2  (172.31.80.31): SUCCESS
        Pinging home3-b eth2  (172.31.80.32): SUCCESS
        Pinging Gateway port  (172.31.80.1): SUCCESS
        Pinging Virtual IP  (172.31.80.30): SUCCESS


Info: Checking DNS configuration.
        Pinging Server Virtual IP DNS (home3.lzsip.com): SUCCESS
        Pinging home3-a DNS (home3-a.lzsip.com): SUCCESS
        Pinging home3-b DNS (home3-b.lzsip.com): SUCCESS


Info: Checking remote maintenance board version.
```

```
        Version [PLEH08B] OK.

Info: Checking remote maintenance board for home3-a.
        Login to home3-a RSA card is successful.

Info: Checking network configuration for home3-b.
4 Network interfaces found. OK.

Number of tests = 12
Number of passed tests =  12
```

5. Enable the loader watchdog on the RSA.

Initial administration for both edge servers and all home servers

The equipment is databased through ART. Once administered, the new passwords and PPP address are provided.

Best practice is to use **Update** on each piece of this installation.

If you complete all the administration and *then* select **Update**, and if the HOST fails, you must remove all of the rest of the database before that piece can be fixed. Update after each piece to avoid this.

The ART script guides the technician through the steps to administer this information.

Follow these steps:

1. After the ccsInstaller script is finished and you have verified that the server(s) are running SES services, ensure that the USB modem is connected correctly to the USB port on the server.
2. The USB modem provides access to the Avaya SES servers so that you may perform basic administration required to configure the server for use. Once the USB modem on the server has been installed and configured, you may dial into it over PPP. To establish this PPP session, you may use either Windows dial-up networking, or the `connect2` tool commonly used by Avaya services personnel.
   a. Ensure that your system environment has been set up for using the tool.
   b. Execute the **`connect2`** command, if available, specifying the phone number to dial, the login and password to use on the server, the terminal type to use for the server, and the password for RAS access:

```
connect2 -p 3035551234 -l admin -c password -t CCS -R rasaccesspassword
```

   c. The system displays various connection-related messages, including the IP address, and then ultimately returns a shell prompt from the remote server that you are accessing.
3. After this remote connection has been established successfully, then:
   a. Open a web browser window and type the following in the URI field:

      http://*`host_name`*/admin

      The *`host_name`* is the fully qualified domain name of the server (if you have DNS administered) or the IP address shown in the preceding `connect2` message.
   b. Enter the default administrative user name admin in the Logon ID field and select Logon.
   c. Enter the initial password for the admin account, and select **Logon** again. Note that after this initial logon, the default password should be changed for security reasons.
   d. At the next screen, select **Launch Administration Web Interface**. You receive a warning about License Error Mode. You may ignore it until after completing the SES system's licensing administration.

e. Select Setup to display the first of theSetup screens on page 159. Select each link on the Setup screen, in turn, to complete the initial server administration screens.

f. From Setup, select Setup Domain. The Edit System Properties screen on page 318 is displayed. Enter the network name or IP address of the domain to which this server is assigned (usually, an enterprise's top level) in the Domain field.

g. Enter the fully qualified domain name or IP address of the server on which you intend to enable the WebLM service for this SES system in the **License Host** field (for example, a home server would enter the name of its edge server) and select **Update**. Note that, for duplexed server configurations, this is the physical fully qualified domain name or IP address of the SES system running WebLM, not the virtual address of the duplex pair.

h. Note at the Continue screen that the proxy service must be restarted on every home server in your system for this domain entry to take effect. (To do this manually, select the Proxy Server's Stop link from the Services Administration screen on page 314, and after confirming that this process has stopped, then select Start.) Select Continue.

i. From Setup, select **Setup Hosts**. The first server you set up must be the edge server. Then set up any other home servers.

   If only the home server is visible from this screen, then the Master Administrator interface is on another machine.

j. On the Add Host screen on page 165, enter the name of the server (for example, edge.customer.com) in the **Host Name** field and select a type from one of the following entries in the drop-down list labeled Host Type.

   - Edge -- An edge proxy server handles SIP requests coming from all domains.
   - Home/edge -- An home/edge proxy serves as both an edge proxy (handling requests from other domains) and a home proxy (handling requests within this domain). If your proxy is an home/edge server, then no other proxies are allowed.
   - Home -- NOTE: This type is available *only* after you have set up the edge server.

k. In the **Password** field, enter the mvss database password that you set during installation.

l. Since only home proxies must designate an edge parent, accept the default **Parent**.

m. Set the **Profile Service Password** for this host.

n. The only link protocol that is supported for SIP trunking in Avaya Communication Manager is TLS. By default, all Listen Protocols and one Link Protocol (TLS, for SES host-to-media server communication) are selected. You may select your own, so long as any link protocol you select is also selected as a listen protocol.

   For example, if you're using a 46xx SIP telephone, or you're connecting to a SIP service provider, then you will probably check all three listen protocols. If you use only the IM client in SIP Softphone R5 within your enterprise, then the TLS Listen Protocol is sufficient.

o. (Optional) When a SIP client tries to register with this host, by default the minimum-duration registration acceptable is 15 minutes. If you wish to change this value, enter a new, whole integer, 900 through 59,940, in the **Minimum Registration** field.

p. (Optional) You may accept or change the defaults for the following fields:
   - Presence Access Policy
   - Minimum Registration (seconds)
   - Outbound Routing Allowed From
   - Outbound Proxy
   - Outbound Port
   - Outbound Transport
   - Outbound Direct Domains

q. Select **Add** and then select **Continue** on the confirmation screen.

r. If you just added the edge server, then repeat the steps to add at least one home server. After you're finished adding hosts, select **Update** on the left-hand side of the screen. All pending updates administered on this host will then be synchronized on all other hosts.

s. (Optional) After you have added at least one home server, select the **Setup Default User Profile** or **Setup Media Servers** link from the **Setup** screen to access the Edit Default User Profile screen on page 172 or the Add Media Server screen on page 174. (NOTE: Completing the latter is required before any media server extensions can be administered.) After these associated screens have been completed, Setup disappears from the left-hand menu of choices.

Note:

After making any changes or additions to server information, always select Update on the left-hand side of any administration screen to send pending updates to all the servers. Selecting Update after completing a set of changes or initial administration ensures that the databases on all servers (or on a single combined server) are kept in sync.

Server license installation

There are three types of licenses. These three licenses are accommodated in one file. Terminology is different between the Master Admin interface License screen and the WebLM->Licensed Products->IMPRESS screen.

See the table below.

Admin Web Interface	Web LM screen
Edge Proxy	Edge Proxy License (EDGE_proxy)
Basic Proxy	Home Proxy License (BASIC_proxy)
Home Seats	Home Seat Licenses (HOME_seats)

The WebLM server is installed in one location only, on an SES edge server. For a duplexed pair, pick an edge server's physical name or IP address, usually the A server.

Obtain licenses for the Avaya SES system with these steps:

1. To obtain the correct MAC address, go to a command line and type `get-mac-address`.

   Alternatively,

   a. Enable and log in to WebLM using steps 5 through 9 below.

   b. Select **Server Properties**. The contents of the **Primary Host ID** field is the eth0 MAC address of the server.

2. Use your established RFA web procedures for obtaining licenses for Avaya servers.

   a. Use the MAC address you obtained in Step 1.

   b. Go to the RFA web site at http://rfa.avaya.com and download the license file to where you can upload it later on, typically to a location on the PC used by authorized services personnel.

3. You must logon and select the link to the Maintenance Web Interface.
4. From the list of available Security screens, select the link to view the WebLM Software screen.
5. If WebLM is not already enabled, select **Enable WebLM**.
6. From the list of available Security screens, select the link to view the WebLM License Administration screen.
7. Select **Access WebLM**.

   The system displays the WebLM application screen.

8. From the WebLM screen, select **License Administration** and then enter the WebLM default administrative password.

9. After your initial log in, the system prompts you to change the password. WebLM logs you out and expects you to log back in with your new password.
10. Select **Install license**.
11. Then select **Browse** and navigate to the location where you saved the license file in Step 2, and then select Install.

    The proxy server will renew acquired licenses every 5 minutes. However, initially, it has not acquired any licenses (there were none installed) so the proxy server will actually be trying every 60 seconds. Then, once it gets them all, it will renew them every 5 minutes.
12. If you need a server to acquire or re-acquire a license immediately, perhaps to update the number of home server seats you are allowed quickly, use these steps:

    a. Restart an Avaya proxy server manually.

    b. From the Master Administration interface, select the **Services** screen, and then select the proxy server's **Stop** link.

       Confirm that this process has stopped, and select the **Start** link.

Administer Communication Manager and endpoints

Endpoints for Communication Manager include a variety of devices, terminals or stations:

- Avaya SIP phones
- Third-party SIP phones
- Wireless, digital, and analog endpoints
- Avaya 46xx Softphone
- SIP Softphone R2 or later
- IP Softphone R5 or later
- Before your installation is complete, you must use the established procedures to administer the Communication Manager media server for use with SIP. These steps include adding users of SIP telephones and Avaya SIP Softphones, adding extensions for each user, and updating proxy route patterns, as appropriate.
- A SIP-enabled station, such as the Avaya 46xx, should be administered in Communication Manager 3.0 as an Off-Premises Station (OPS). See the *Avaya Extension to Cellular and OPS Installation and Administration Guide*, Issue 6 or later.

Follow these steps:

1. Administer Communication Manager to work with SIP devices.

   The fields that differ SIP from non-SIP Communication Manager media server setup are detailed in *SIP Support in Avaya Communication Manager*.

   The document includes entries for Signaling Group and Trunk Group setup that are specific to SIP. After you have completed setup in Communication Manager, perform a **Save Translations** to save changes.

2. Set up the telephones and endpoint devices.

   After setting up Avaya SIP Softphone users in Communication Manager as SIP Softphones on (OPTIM/OPS), ensure each client PC has the proper release of Softphone software installed, licensed and configured to use SIP for Instant Messaging (IM). Refer to online help in the SIP Softphone application for more information. You also may wish to verify that these softphones can register with the edge/home, and then can send and receive instant messages, update their contact lists, and so on.

3. Check the endpoint devices

   After administering SIP telephones in Communication Manager, ensure that each telephone has a version of firmware that can support SIP. Note that the Avaya 46xx SIP telephone ***requires*** that you enter a domain name on its SIP Settings page. You may wish to make and receive test calls, too.

For application notes on which third-party SIP endpoints are supported, go to the web site:

`http://www1.avaya.com/enterprise/resourcelibrary/applicationnotes/` and then select the link for **Network Infrastructure** under **DevConnect Product Integration**.

Change the DNS name

This procedure provides two ways to change the DNS name of your system.

The best way is to do a full reinstall, and answer the DNS question with the new name.

A shorter, but only partially tested procedure is this:

1. Take the B server out of service.
2. Shut down the B server.
3. On the A server, execute the command **`service postgresql stop`**
4. Run ccsInstaller on the A server.
5. Answer **y** when ccsInstaller asks **Do you want to stop the watchdog?**
6. Complete the ccsInstaller prompts on the A server.

   The services are still off.
7. Power on the B server.
8. Repeat steps 4, 5 and 6.
9. Execute the **`in-service`** and **`reboot`** commands on both A and B servers.

Chapter 8: Administration web interface

This section describes in detail the use and meaning of the screens in the Master Administration interface. This topic is divided into groups, based on the main headings in the menu at the left of the main window.

Publication Note

Most of the screen examples in this document were taken from a combined home/edge simplex server. If your installation is any other configuration, the screens may slightly differ. Figures are taken from other hardware configurations only in instances where a duplexed pair or multiple home servers were needed for example.

Top Screens

These screens are the first ones you use when you log on.

- Logon screen on page 156
- Logon screen field descriptions on page 157
- Choose Interface screen on page 158

Logon screen

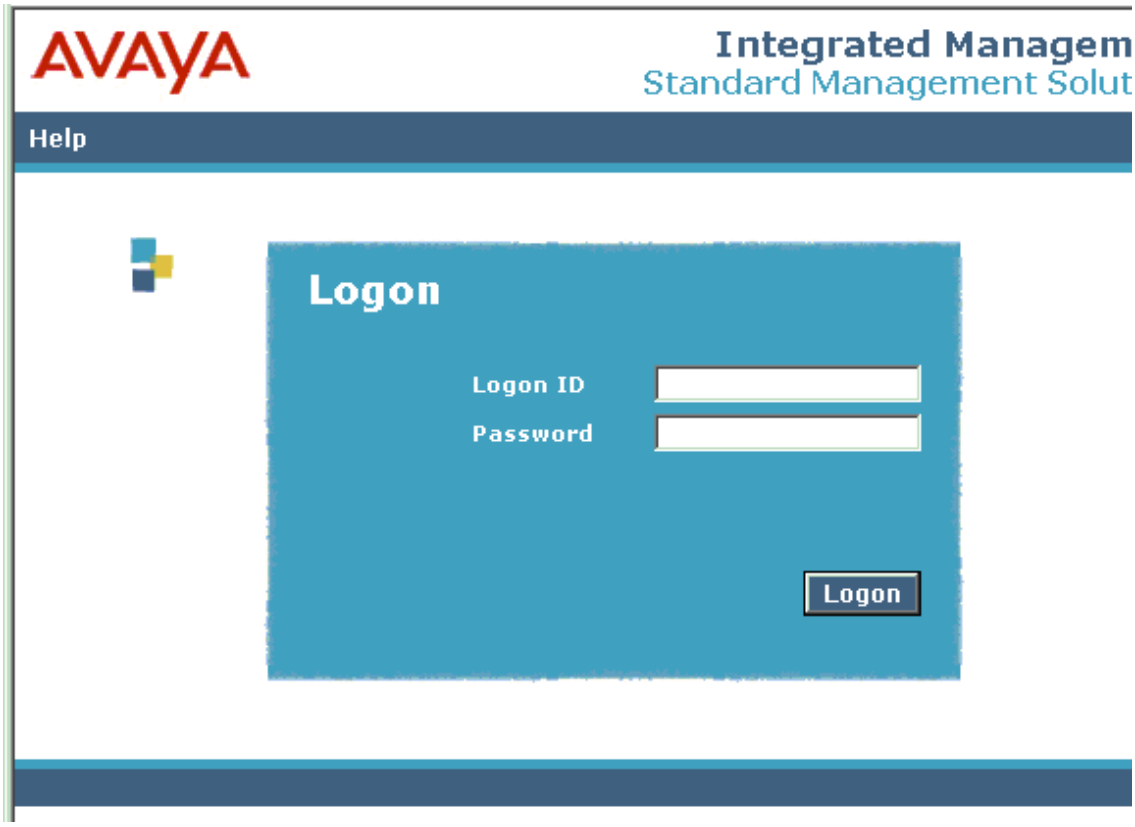
To display the Logon screen, enter this URL:

https://123.45.67.89 /admin

The URL for the SIP PIM application that an end user sees, is this:

https://123.45.67.89/

Figure 15: Logon screen



Logon screen field descriptions

Logon ID

(Required) Enter the user name with which to log on to your administrative account. After you enter this and press the Enter key or select **Logon**, the screen refreshes with the **Password** field.

Password

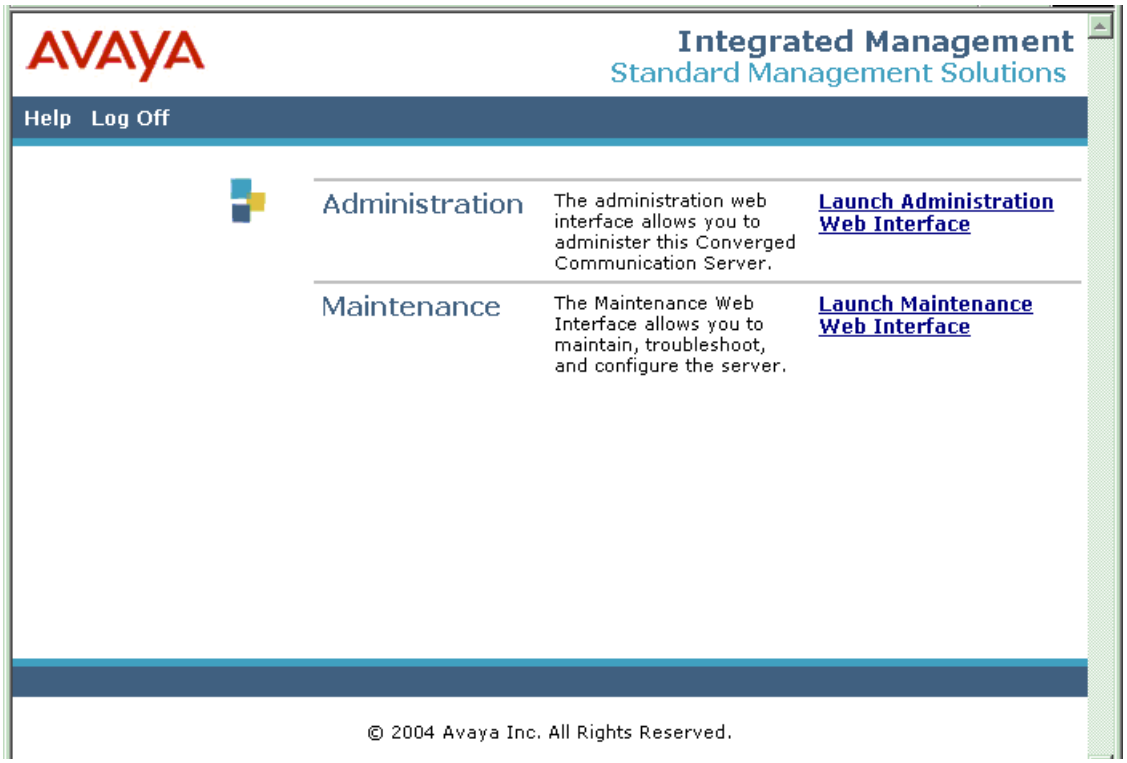
(Required) Enter your administrative account's password, at least 6 characters in length, at least 1 of which is alphabetic and at least 1 numeric.

After completing both fields, select **Logon** or press Enter.

Choose Interface screen

Use the **Choose Interface** screen after logging on to select from either the Administration Web Interface or the Maintenance Web Interface, depending on what functions you need to perform on the server.

Figure 16: Choose Interface screen



Choose Interface screen field descriptions

Administration

The administration interface provides screens for initial server setup, user contact database changes, and media server-related activities. Select the link to the right to **Launch Administration Web Interface**.

Maintenance

Maintenance activities include server status and diagnostics, alarms and traps, and remote access security. Select the link to the right to **Launch Maintenance Web Interface**.

Setup screens

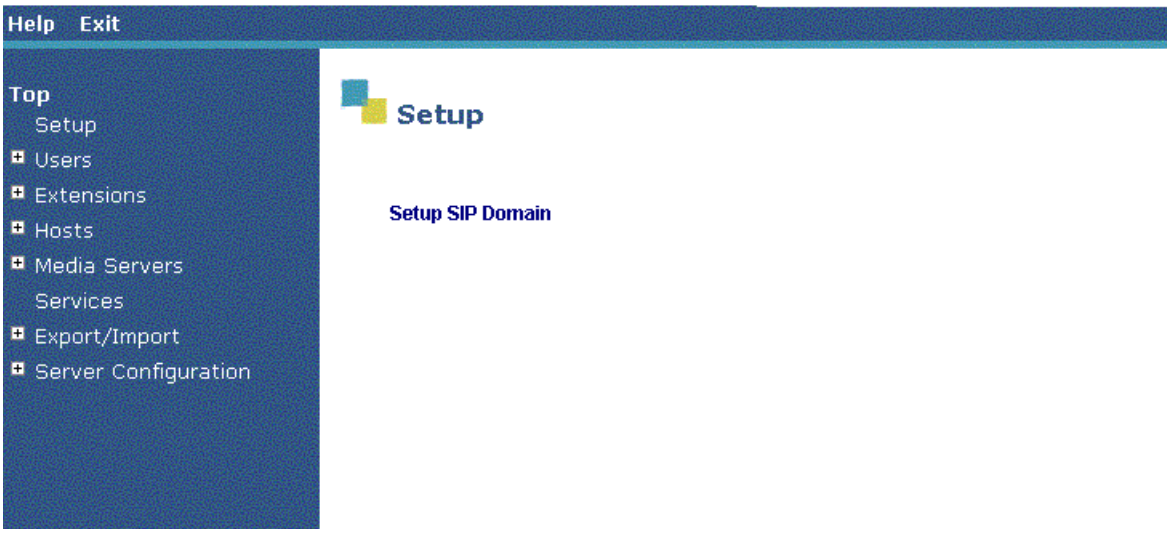
When installing or updating, the setup screens provide the needed interface. Once the system is set up, these screens are available individually, but not displayed by the system as a setup task. The setup screens consist of these:

- Setup screen on page 159
- Edit System Properties screen on page 163
- Add Host screen on page 165
- Edit Default User Profile screen on page 172
- Add Media Server screen on page 174

Setup screen

The **Setup** screen contains links to the screens necessary to configure servers for initial use. This screen provides different choices, depending on which required tasks have been completed. The first **Setup** screen is shown in Figure 17.

Figure 17: Setup SIP Domain screen



Before filling in the Setup screens, you need to know IP addresses, machine names, and answers to the prompts in the install script. See Worksheet for Duplication on page 461 for a list of the things you will need to know.

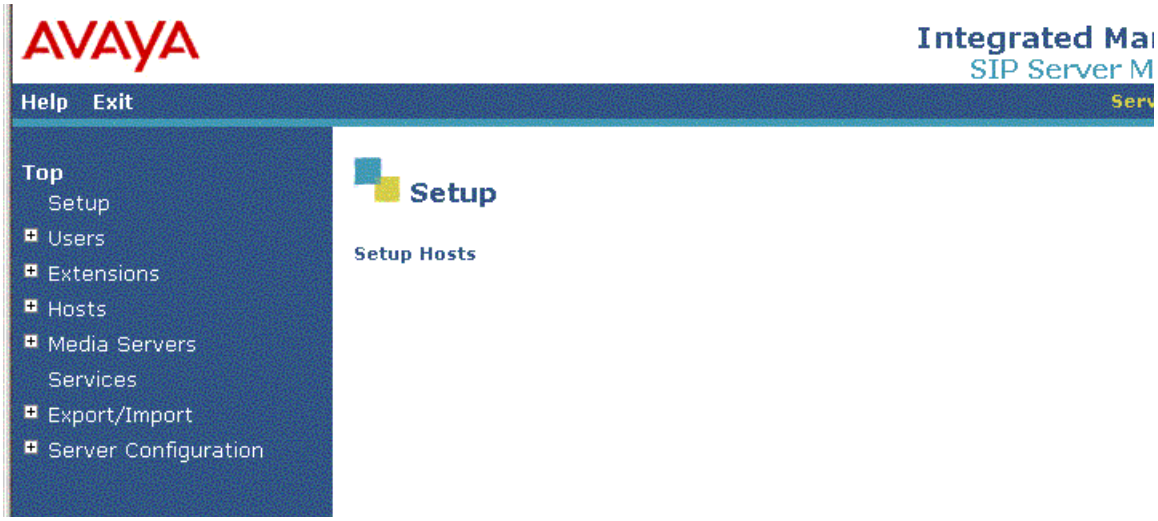
Setup screen field descriptions

Setup SIP Domain

Select this link to go to the Edit System Properties screen on page 163. You must specify the domain to assign to this SES configuration before you may proceed with any other setup options. You must restart the proxy service on each SIP proxy host computer in your enterprise before any newly specified domains are recognized system-wide. From the Services Administration screen on page 314, select the **Stop** link for the Proxy Server, visually note that the process stopped, and then select the **Start** link.

The next Setup screen lets you set up your host:

Figure 18: Setup Hosts screen



Setup Hosts

After setting up the domain, select this link to create a host computer entry for the servers in your enterprise. Recall that a host is either a home, an edge, or a combined home/edge. The link on this screen directs you to the Add Host screen on page 165.

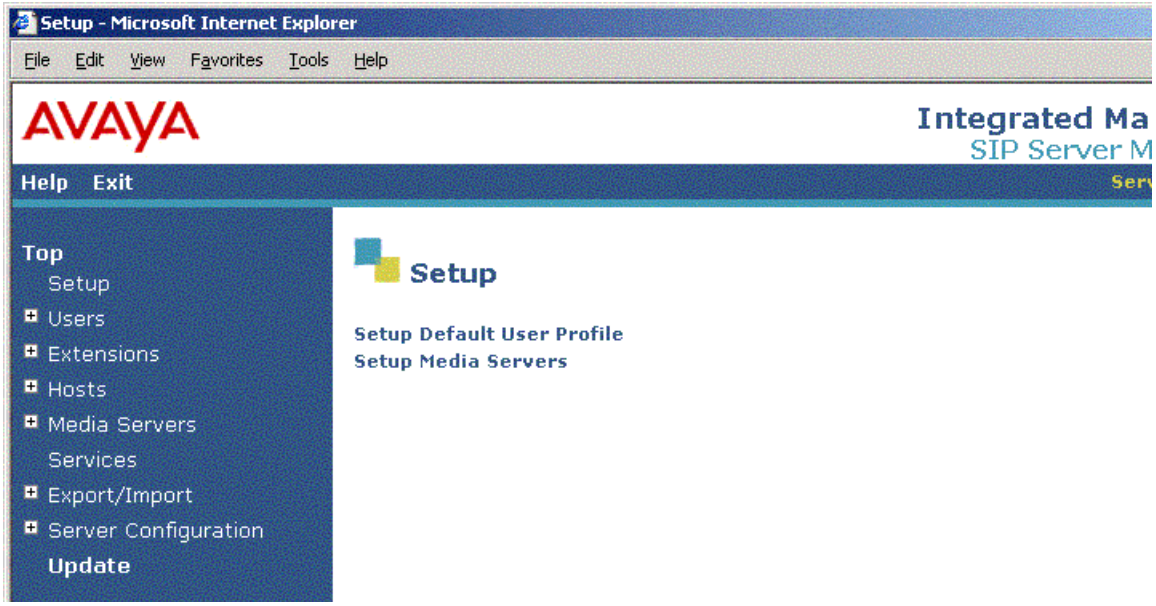
Note:

You will not be able to continue with administration and configuration until these first two Setup options (at a minimum) have been completed.

The next **Setup** screen typically provide two other choices. Completing these screens is optional but recommended before continuing with end user or telephone number extension administration.

Be aware that you may not add user information or media server extensions until the next two setup options are completed.

Figure 19: Setup Default User Profile and Media Servers screen



Setup Default User Profile

The system displays this link after you have added at least one home or exactly one home/edge server with **Setup Hosts**. Now, you may select this link to go to the Edit Default User Profile screen on page 172 or you may first choose to set up your system's media servers running Communication Manager.

Information for user profiles now accepts UTF-8 encodings to accommodate multibyte languages. You may input Shift_JIS (SJIS) as well. Whether the user's browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

Setup Media Servers

This system makes this link available after you have added any type of host using the **Setup Hosts** link. Select this link to go to the Add Media Server screen on page 174 where you create one or more entries for your network's media servers running Avaya Communication Manager.

Media gateways must also be up-to-date.

Tip:

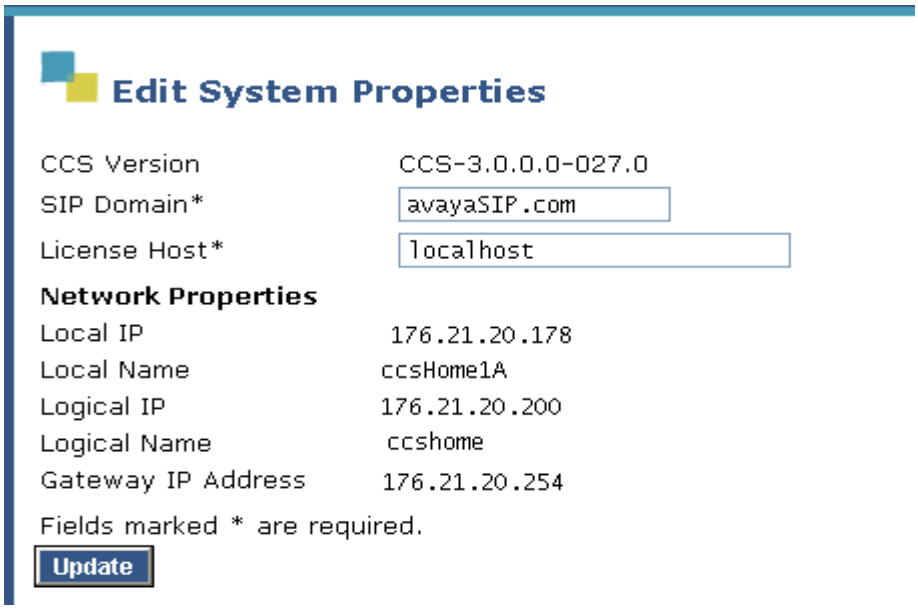
Note that you may not add user information (for example contacts) or media server extensions (telephone numbers) to the database until these setup options have been completed.

Edit System Properties screen

The Edit System Properties screen defines the server's domain.

Note that in Figure 20, the local and logical IP addresses differ, indicating that this is a a duplexed home configuration. The network properties were provided at installation time.

Figure 20: Edit System Properties screen



Edit System Properties screen field descriptions

CCS Version

(Read Only) This field displays the major and minor release number (R3.0.0.0) and the current load and build number, 27, of the Avaya software that is running on this SES server.

SIP Domain

(Required) Enter a domain name to assign to this SIP Enablement Services system.

Note:

Updates to system-wide properties like the **SIP Domain** field require you to restart the proxy service on each SIP host computer in the system. Otherwise the updates are not recognized.

License Host

(Required) Enter the host name, the fully qualified domain name, or IP address of the SIP proxy server in your Avaya system that is running the WebLM application and has the associated license file installed.

This entry should always be **localhost** unless the WebLM server is not co-located with the SES hosts. If not co-located, put the IP address of the licence host in this field. Note that, for duplex-server configurations, this is the physical, fully qualified domain name or IP address of the SES system running WebLM, *not* the virtual address of the duplex pair.

Network Properties

(Read Only) Lists the Local IP address and Local Name for this physical server, as well as the Logical IP and Logical Name for this node.

Local and Logical properties are the same for each server in a simplex configuration.

On a server that is one of a duplex pair, its Local properties differ from its Logical ones. However, the Logical properties are the same for both of the servers of a duplex pair.

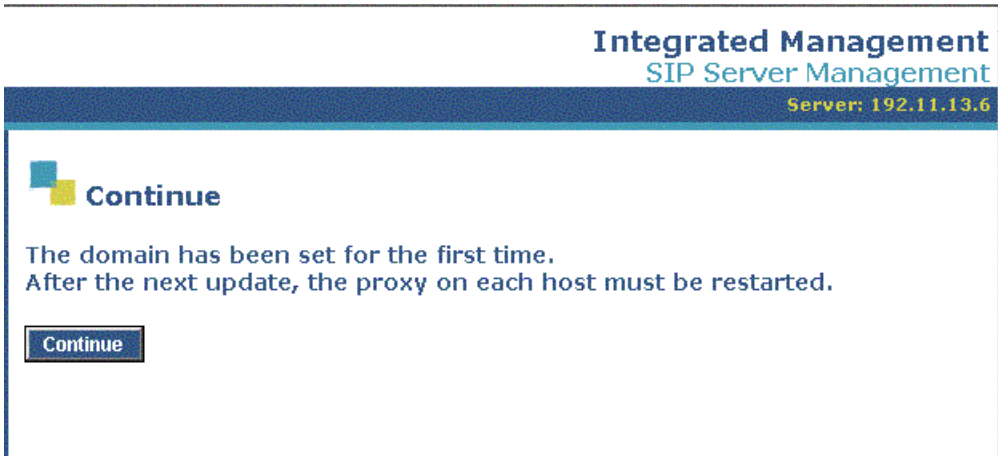
RSA Properties

The system displays this field only if the hardware platform is an Avaya S8500.

(Read Only) Lists the Gateway IP Address and RSA Host Name for the RSA module in this host. Note that this information cannot be changed from within this Administration web interface. Connect to the RSA device and work through that.

Select **Update** to submit the updated information on this host. Then all the hosts should be updated.

Figure 21: Setup Continue screen



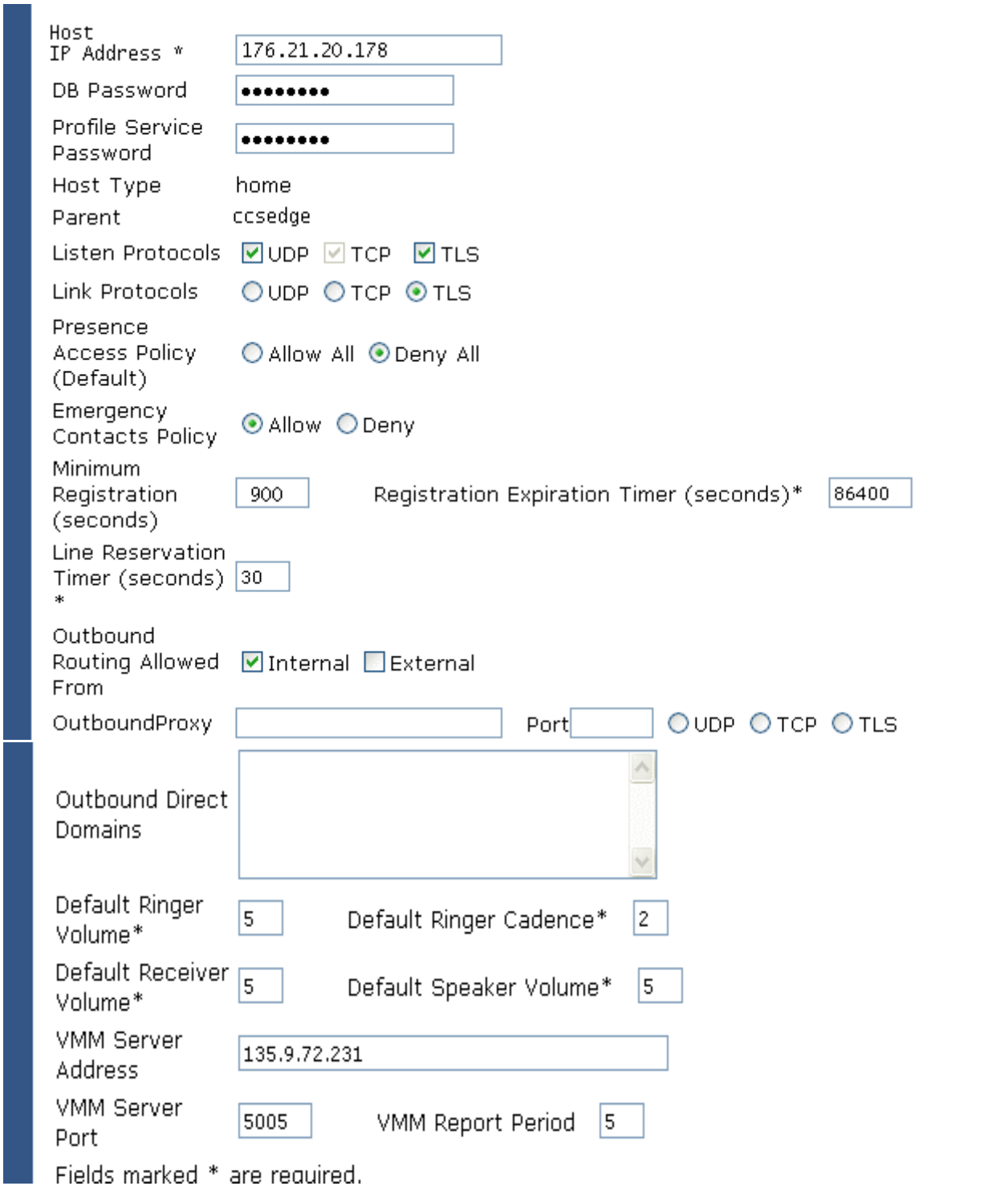
Add Host screen

A host is a home or edge server, or a combined home/edge server.

If your system architecture uses a simplex home/edge architecture, you cannot add a host of any kind, and are denied access to this screen.

If your system architecture is a single edge server with one or more home servers, use this screen to add the edge server, and then add each home server. Specify the type in the **Host Type** field.

Figure 22: Add Host screen



Add Host screen field descriptions

Host IP Address

(Required) Enter the IP address for this host server, either home, edge, or home/edge.

DB Password

(Required) Enter the password assigned to the database at installation. This password should be at least four alphanumeric characters in length.

Profile Service Password

(Required) This password provides permissions between the SES hosts, both home server and edge server.

The Profile Service Password is not used by users or administrators. Rather, it is a password that uniquely identifies a proxy for intra- and inter-proxy communication. The Profile Service Password must be unique for each administered host.

Host Type

(Required) Select one of the following from the drop-down list:

- Edge—if this will be an edge proxy server for the SIP traffic of all domains.
- Home —This option appears only after an edge proxy has been added. If this will be a Home proxy to manage the SIP traffic of a specific domain.
- Home/edge—if this server functions as both your enterprise's edge and home proxies. Note that no additional proxy servers may exist within this architecture.

Parent

(Required) Select one of the following from the drop-down list to indicate the media server this host uses:

- Select NONE if you selected edge or home/edge for the server's Host Type, above. An edge server has no parent.
- Select HOST NAME or IP if you selected home for the server's Host Type field above. the name of the edge servers or CLANs for all your enterprise's domains are listed. Select the correct edge server as Parent.

Listen Protocols

At a minimum, select TLS for the **Listen Protocol**. You may select UDP or TCP for other uses, but Avaya Communication Manager only supports the TLS link protocol for SIP trunking.

Note that the protocol you select for linking must also be selected here for listening. At a minimum, you must select the protocol you selected as the **Link Protocol**, below, although you may want to select additional protocols only for listening but not for linking.

When you add a host, all three protocols are selected for listening. There is little reason to change this default.

Link Protocols

This field refers to the trunk signaling between the Converged Communications Server R3.0 and Communication Manager. Typically, the selection here matches the Signal Group value on Communication Manager.

The only link protocol that is supported for SIP trunking with Avaya Communication Manager is TLS. For third-party proxy servers, you may select to link to SES with TLS, TCP, or UDP, although UDP is untested at this time.

You must also select the Link Protocol as a Listen Protocol, above. You may want to select additional listen protocols.

All three protocols are selected by default and available. There is no special reason to change the default.

Presence Access Policy

This setting correlates to the Watcher feature on the end user's SIP PIM web interface.

Accept the default policy of **Deny All**, or select **Allow All** to change this default policy and show the presence of SIP users on this server. The system displays the presence of SIP users on the SIP PPM web interface and on the Watchers screen.

The administrator may set a system policy to specify that all users on the system default to a blocked state, where users must authorize each other to view each other's presence. This may be overridden by the user's policy.

This administration policy is on a per node basis and may be administered for each home node in the network.

Emergency Contacts Policy

Enable this field to allow unauthenticated calls for the emergency contact named for this host.

If you allow emergency contacts, emergency calls can come to this host.

If you disable this field, unauthenticated calls to emergency URIs will be dropped.

Set up emergency URIs for the end user with the Add Emergency Contact screen.

Minimum Registration (seconds)

Enter a whole number of seconds, 900 through 59,940, that the SIP server should consider as the minimum acceptable duration value when a SIP client registers. If no value is entered, the default of 900 seconds will be used.

Registration Expiration Timer (seconds)

The value for Registration Expiration Timer determines how long a SIP endpoint should register for and renew its registration.

This value is not enforced by the registrar, but downloaded by an endpoint through PPM if they support it. The minimum registration time is enforced by the SIP registrar and it will not allow new registrations prior to that minimum registration time.The minimum registration timer is a SIP protocol feature that prevents endpoints from registering too quickly. Such a registration may be in error.

The default is 3, 600 seconds or 60 minutes.

This field affects all the users on this host.

Line Reservation Timer

(Required) This value is used to configure the maximum amount of time that an end user is allotted to dial a number after going off-hook. The default for this field is 30 seconds. The range is 30 to 240 seconds.

Outbound Routing Allowed From

Select **Internal** or **External** or both to specify whether SIP traffic can be routed only from endpoints internal to this server's domain, or also from those external to it.

Outbound Proxy

Enter the hostname of the server within your enterprise that should manage SIP traffic bound for domains external to this server's domain. For example, on a home server, this would be the hostname of the edge that serves that home. On an edge/home or edge proxy server, an entry in this field typically is not required.

This field can contain the IP address of an edge for alternate use by a home.

Outbound Port

Enter the number of the port (1-65535) on the outbound proxy server specified above that should manage SIP traffic bound for domains external to this server's domain. **Port 5060** is recommended if the entry for Outbound Transport is TCP and **port 5061** if it is TLS.

Select the transport protocol of the outbound proxy server that should manage SIP traffic bound for domains external to this server's domain. Use TLS as a best practice.

Outbound Direct Domains

Users do not need to be under the same edge to take advantage of hairpin and the absence of map addresses. For example, a user in New York can call another user in Paris, and the call is directly routed to the trusted domain in Paris. Set those trusted domains for the host, home, edge, or home/edge, here.

Use this area to list those domains for which traffic may completely bypasses the Outbound Proxy server specified above. Separate entries in the list with commas, or with a white space followed by a new line, after each domain.

Select the **Add** button to add a host with the properties you've entered. If you have added an edge proxy, then selecting **Continue** at the next screen returns you to the Add Host screen on page 165 until you add home proxy as well. If you add a combined home/edge proxy, then you return to the Setup screen on page 159.

Default Ringer Volume

(Required) This field sets the ringer setting for the stations bridged appearance buttons. The values in this field are not related to the ringer setting configuration in Communications Manager, nor does it reflect the Communication Manager's settings.

The default is 5. The range is 1 to 10.

Default Ringer Cadence

(Required) The value in this field sets the speed of the ring tone for the user you selected in the List Users screen. The default is 2, the range for this field is 1 to 3.

Default Receiver Volume

(Required) This field sets the volume in the handset, rather than the speaker. The default is 5. The range is 1 to 10.

Default Speaker Volume

(Required) This field sets the volume on the speaker rather than the handset. The default is. The range is 1 to 10.

Voice Over IP Monitoring Manager (VMM) is a voice over IP (VoIP) quality of service (QoS) monitoring tool. This feature is available only on TSP SIP phones, model SP-1020A.

VMM information is taken from the VMM server. SES requires the server name, port address, and how frequenly an end point should report back to the VMM Server. See the VMM document Voice Over IP Monitoring Manager User Guide 555-233-510.

VMM Server Address

Address of the VMM server.

VMM Server Port

Port number for the VMM server’s address.The range is 1 through 65,535, and the default is 5005.

VMM Report Period

The report period is in seconds, and reflects how often an end point should report back to the VMM server. Reports show jitter, round trip time, and packet loss. This may help in solving troubles on the SES network. The range is 5 through 30 seconds, and the default is 5 seconds.

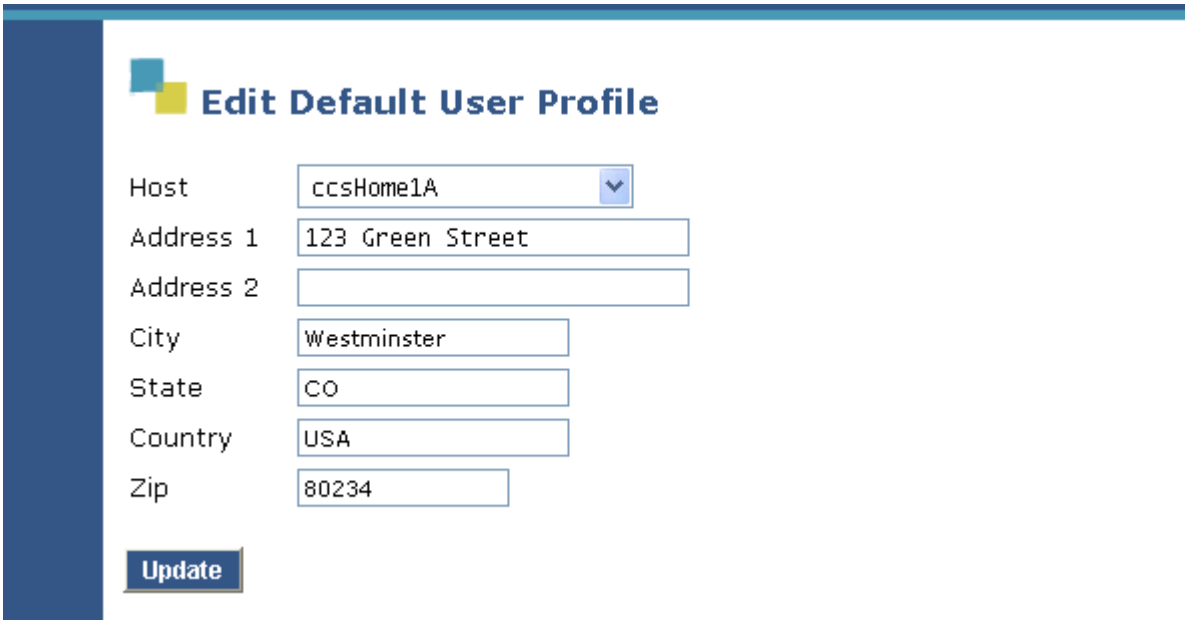
Edit Default User Profile screen

This screen lets you enter a common address for all user profiles on the SIP system. You will not have to type it in repeatedly for each user later. The system displays the data you enter here on an individual user's profile. You can change it there to be more specific.

There is exactly one default user profile on the entire system. The default user profile data resides on the edge server. If you administer the default user profile, an optional task, that one profile populates all user profiles. A specific user's profile is then pushed to their specific home.

Information for user profiles now accepts UTF-8 encodings to accommodate multibyte languages such as Japanese. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

Figure 23: Edit Default User Profile screen



Edit Default User Profile screen field descriptions

Host

From the alphabetized drop-down list of names, select the name of the home server for whose users this location information will become the default entries. The host name selected by default in the list is either the first home server alphabetically or the single home/edge server.

Address 1, Address 2

This is the first line and second line of the default address for users. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

The name will be assigned to the speed dial button for this contact. In Japanese, this name string uses Kanji characters. (Contrast this with Alias).

City

Enter the name of the city or town of the default address for users. You may use alphanumeric characters.

State

Enter the name of the state or province of the default address for. You may use alphanumeric characters.

Country

Enter the name of the country of the default address for users. You may use alphanumeric characters.

ZIP

Enter the ZIP or postal code of the default address for users. You may use only numeric characters.

Edit Default User Profile screen commands

Update

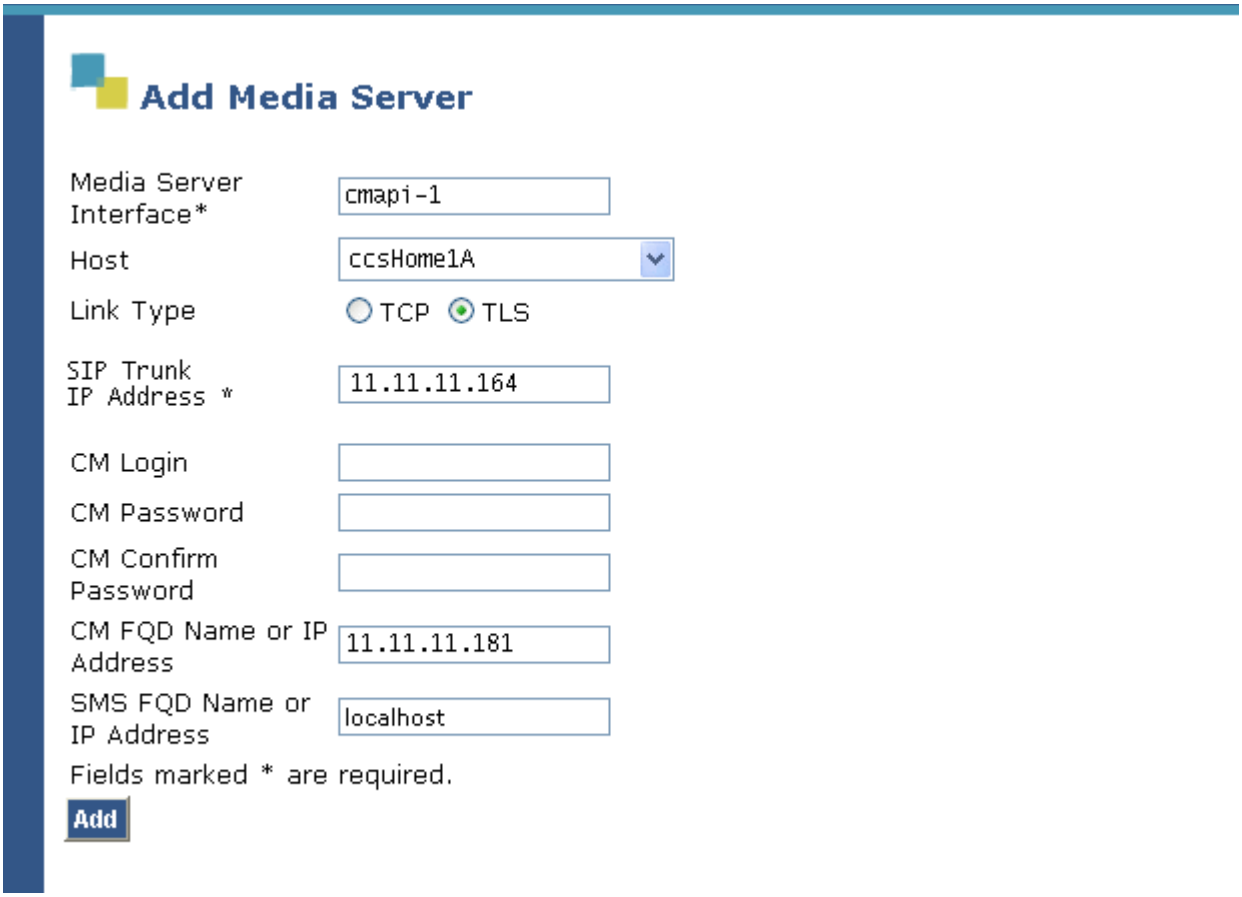
Select **Update** to submit the information on this screen to the server's database. The system displays a Continue screen so that you can click Continue. The system displays the User Administration menu screen.

Add Media Server screen

This screen assign a home servers to a media server interface.

If you are administering SIP trunking on your media server running Communication Manager, use this screen to add that SIP-enabled media server to the SIP domain and correlate it to a home server.

Figure 24: Add Media Server screen



Select **Add** to submit the media server with the properties entered to this database for this home host.

Add Media Server screen field descriptions

Media Server Interface

(Required) Enter a friendly name in alphanumeric characters referencing the CM media server's CLAN (or processor CLAN) IP interface. You may wish to use the same name as is used for this media server on the IP Node Names screen in Communication Manager. Each CM media server's name must be unique. Refer to "Administration for Network Connectivity for Avaya Communication Manager," Doc ID 555-233-504.

If the media server has more than one interface present, you must address each interface separately.

Host

(Read Only) From the alphabetized drop-down list of names, select the name of the home server that you want to associate with the Communication Manager media server's SIP trunking. The edge host name selected by default in this list is that of either the first edge server alphabetically, or the single home/edge server.

Link Type

Select one of the listed protocols to link the media server with the specified host:

- TCP (Transport Control Protocol)—if this protocol is not an option for your system, then the Link Type field may not appear on this screen.
- TLS (Transport Link Security)—this is the default protocol which is selected for all servers.

SIP Trunk IP Address

(Required) This field holds the IP address for the media server's CLAN. This field names the link that supports the SIP trunk. The IP address must be specified as a 32-bit address comprising four 8-bit octets (for example, 'xxx.xxx.xxx.xxx' where 'xxx' is a value of 0-255) . If DNS is available within its domain, the fully qualified domain name of the media server's CLAN (or processor CLAN) may be entered.

CM Login

Login for the Communication Manager software. Your login should be of type **customer** and service level **superuser** at a minimum. Understand that this has to be set for every media server running Communication Manager.

CM Password / CM Password Confirm

Password for the Communication Manager software.

CM FQD Name or IP Address

The IP address or the fully qualified domain name, or the native NIC or other administered interface in IP services form on the Communication Manager's CLAN or processor CLAN of the server that holds Communication Manager. This field is for the link that supports SAT commands with the media server's name.

SMS FQD Name or IP Address

The IP address or the fully qualified domain name of the systems management server. SMS is known at Avaya as Integrated Management System (IMS).

IMS monitors the health and alarms of all machines associated with it.

For this field enter localhost, as shown in Figure 25.

User screens

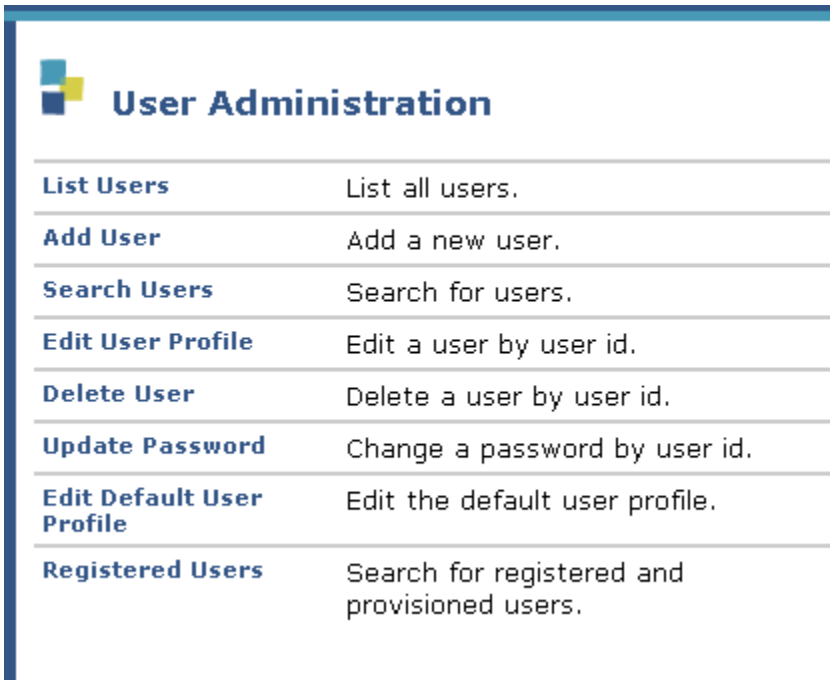
The User screens permit customizing aspects of the system for each user.

User Administration screen

Select Users on the menu in the left of the window to display this screen.

This screen presents differently if you are using the Limited Administrator interface on a home server. All of the options listed below are not available.

Figure 25: User Menu screen



User Administration screen descriptions

Information for user profile screens now accepts UTF-8 encodings to support multibyte languages such as Japanese. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

List Users

Select this link to go to the List Users screen on page 180 and view all users administered in the database. As a result of a search, this list may have one or several users showing.

Add User

Select this link to go to the Add User screen on page 237 and create a database entry for a new user.

Search Users

Select this link to go to the Search User screen on page 241 to use entries in the database as search criteria to find one or more users' profile(s).

Edit User Profile

Select this link to proceed to the Edit User Profile screen on page 248 and enter a user ID for the user whose profile you wish to modify. Note that this will modify only the selected user's profile, not the default profile for new users.

Delete User

Select this link to proceed to the Confirm Delete User screen on page 252 and delete a single user. Type a user ID for the user you want to delete. Confirm your deletion on the next screen.

Update Password

Select this link to proceed to the Update Password screen on page 246 and enter a user ID for the user whose password you want to change.

Edit Default User Profile

Select this link to go to the Edit Default User Profile screen on page 172 and modify one or more entries. This will modify the default values to be populated in the profiles of all users created. Every user's profile reflects what you type here.

View Registered Users

Select this link to go to the Registered Users screen on page 253 and view those users that have SIP clients that have registered to, or been provisioned on a specific home or home/edge.

The View Registered Users screen appears on the home server's Limited Administrator interface as a view only screen.

Note:

The system displays provisioned users only if they are administered as a user and are associated with a media server extension.

The system does not display configured users unless they have been provisioned.

List Users screen

A typical **List Users** screen is shown below. To use this screen, check the box next to a user ID, select an action from the task drop-down menu, select Submit.

This screen is viewed only from the edge's Master Administrator interface.

Figure 26: List Users screen

List Users screen field descriptions

User ID

(Read Only) Lists the IDs of administered users in the database.

Host

(Read Only) This is the name of the home server for this user. A user's host is a home server or a combined home/edge server.

Name

This is the name of as many as 64 UTF-8 characters associated with this User ID and Handle in the user database. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

The name will be assigned to the speed dial button for this contact. In Japanese, this name string uses Kanji characters. (Contrast this with Alias).

List Users screen commands

All of the tasks in this drop-down menu reflect data that the user sees as well on the SIP PIM interface.

You may select any of the tasks in the Task field:

Add User

Use the Add User screen on page 237 to add a new user to this home server. This command is the same as selecting **Users** > **Add** from the menu.

Contact List task

This series of screens relates to the sites and friends the end users want to contact. Create and edit the personal contact with whom this user may want to communicate with the Contact List task on page 185.

Devices task

Manage the tones, volume, and cadence of certain SIP-enabled devices with the Devices Screen menu on page 205.For you to view this screen, the end user must have a compatible device. If you select a user that does not have a device that is compatible with this feature, the system displays Figure 27. This screen indicates that the end user's telephone does not support the Devices feature.

Figure 27: No compatible devices screen

Extensions

Add, delete, and free extensions assigned to a user with the Extensions task on page 214.

Handles

The Handles task concerns how the end user wants to be contacted. Administer a user's personal points of contact, and user groups with the screen in Handles task on page 216.

A user may have more than one handle. For instance, one handle may be the user's media server extension. Another handle maybe a team designation such as Head_Of_Payroll. Even though the number of contacts to a handle is limited to two, the number of handles for a user is *not* limited. A user must always log in to their SIP device using their primary handle as their user ID. A primary handle matches the User ID.

Memos

Write short notes about the user for other administrators to read using the User Memos screen on page 230. Maximum size of the notes is 256 characters.

Profile

Edit the full profile of a user and customize it with the Edit User Profile screen on page 248.

Permissions

Use this task to specify if other SIP users can detect your presence on the system. Selecting this task displays the Permissions screen on page 232.

Watchers

This task choice lets you select for the user who on the system may observe the user's presence. Selecting this task displays the screens for the Watchers Task on page 235.

Submit

Check mark a user, or in limited instances, several users, select a task from the drop-down menu, then select Submit to proceed to the next screen.

Delete

Select this and confirm your decision to delete a user on to the Confirm Delete User screen on page 252.

Delete more than one user at a time by checking several check boxes. You can check up to 68 check boxes to delete up to 68 users at one time.

Move User

Move User occupies the screen only when there is more than one home server. Move User changes a user from one home server to another. See Moving a user to another home server on page 251.

Moving a user to another home server

In this procedure, the destination home server is fully functional.

If you are moving a user to another home server, and that home server is associated with two or more media server interfaces, you will be prompted to select one of those interfaces.

If the user has a media server extension and the destination home does *not* have an administered media server, the Move User operation cannot be completed. The move may only be completed if a media server is added to the destination home or the user's extension is removed or freed.

1. From the Master Administrator interface, go to the List Users screen.
2. Select the check box next to the user you want to move.
3. Click the **Move User** button.

   The system displays a Move User page.

   Select the new home server using the **New Host** drop-down box.

   Only those homes that the user can be moved to are displayed in this box. All home servers that exist are not shown. The **New Host** drop-down box does not contain the user's current home.

   If a home server connects to a media server that contains more than one media server interface, the drop-down menu displays both interfaces for you to choose from.
4. Press OK or Cancel.

   The update procedure is performed by the system.
5. On Communication Manager, change the SIP trunk for the extension of the user.
6. On the Toshiba Business Phone, log out and log in.

See also **Edit User Profile** screen on Moving a user to another home server on page 251.

Contact List task

This series of screens relates to the sites and friends the end user wants to contact. The contact address can be IP addresses, e-mail address, or web pages that an end user would like to communicate with.

In Figure 28, the first four items are common endpoints the user frequently contacts. Group1 is a collected set of endpoints that can be contacted by communication with the group's handle.

This screen is available on the web page viewed by the user, the SIP Personal Information Manager pages, but rendered differently.

Figure 28: My Contact List screen

Contact List screen field descriptions

Handle

This is a valid name or User ID for the contact. Selecting this link displays the detailed user contact information for the contact this user communicates with. Handles must be unique contact URIs within the SES system domain, but contacts may have multiple valid handles.

Note:

The SES system automatically appends the *systemdomain.com* portion of the handle. This portion of the handle should not be entered as part of the handle field when adding or updating a handle.

If you select a user's option button, or select a group name by clicking on it, the system displays a Contact Details or Group Details screen. These two screens let you edit the details about the contact.

Name

(Read only) This is the name of as many as 64 UTF-8 characters associated with this User ID and Handle in the user database. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

The name will be assigned to the speed dial button for this contact. In Japanese, this name string uses Kanji characters. (Contrast this with Alias).

Alias

Displays the optional alias name of as many as 32 UTF-8 characters associated with this contact in the user database. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

In Japanese, this alias string is in Kana characters, and it is designed to help with contact sorting. (Contrast this with Name).

Telephone #1 / Telephone #2

(Read only) Lists a phone number or valid SIP user address, for example, contact Uniform Resource Identifiers (URIs) beginning with **sip:** or **sips:** and associated with this contact's handle in the database. This field may contain a maximum of 256 ASCII characters.

My Contact List screen commands

View

(Read only) View details about the contact or group.

Delete

Select a contact, then select Delete to remove that contact from the user's list. This does not delete the contact from the system.

Add Contact

Add another individual contact or group.

Add Group

Add a group name to which this contact belongs.

Speed Dial

(Read Only) Select this to view the speed dial telephone numbers and speed dial digit assignments for contacts this user may want to communicate with.

Reload Configuration

If you have made changes on this end user's list of contacts, select Reload Configuration to refresh the list.

For SIP users, you may wish to reload the configuration data for your phone, like its Ringer Settings, its Speed Dial List entries (from My Contact List), and its One Touch Dial List entries. Select this link and then submit the reload request.

For system administrators, a variety of data affects the device:

- Changes to network node information
- Data regarding station aliasing
- Associated Dial Plan assignments

These data may have been updated and submitted on the media server running Avaya Communication Manager. Submitting this request reloads this updated device configuration data.

Note:

Provisioned users who have been administered may not have logged on to their device, registering it with the SIP proxy server. Submitting the Reload Device Configuration (or executing the Reload Complete task) will take effect the next time they log on successfully to their SIP device.

When you are ready to reload your configuration for this device, including any station-affecting changes made in Avaya Communication Manager running on the media server, then select the Submit button on this screen. Otherwise, select the Cancel button to ignore this request.

Contact Details screen

This system displays this screen when you select an item and then the View button on the My Contacts screen. This screen is read only. To make changes, select Update Contact to obtain an editable view.

Figure 29: Contact Details screen

This screen is view only.

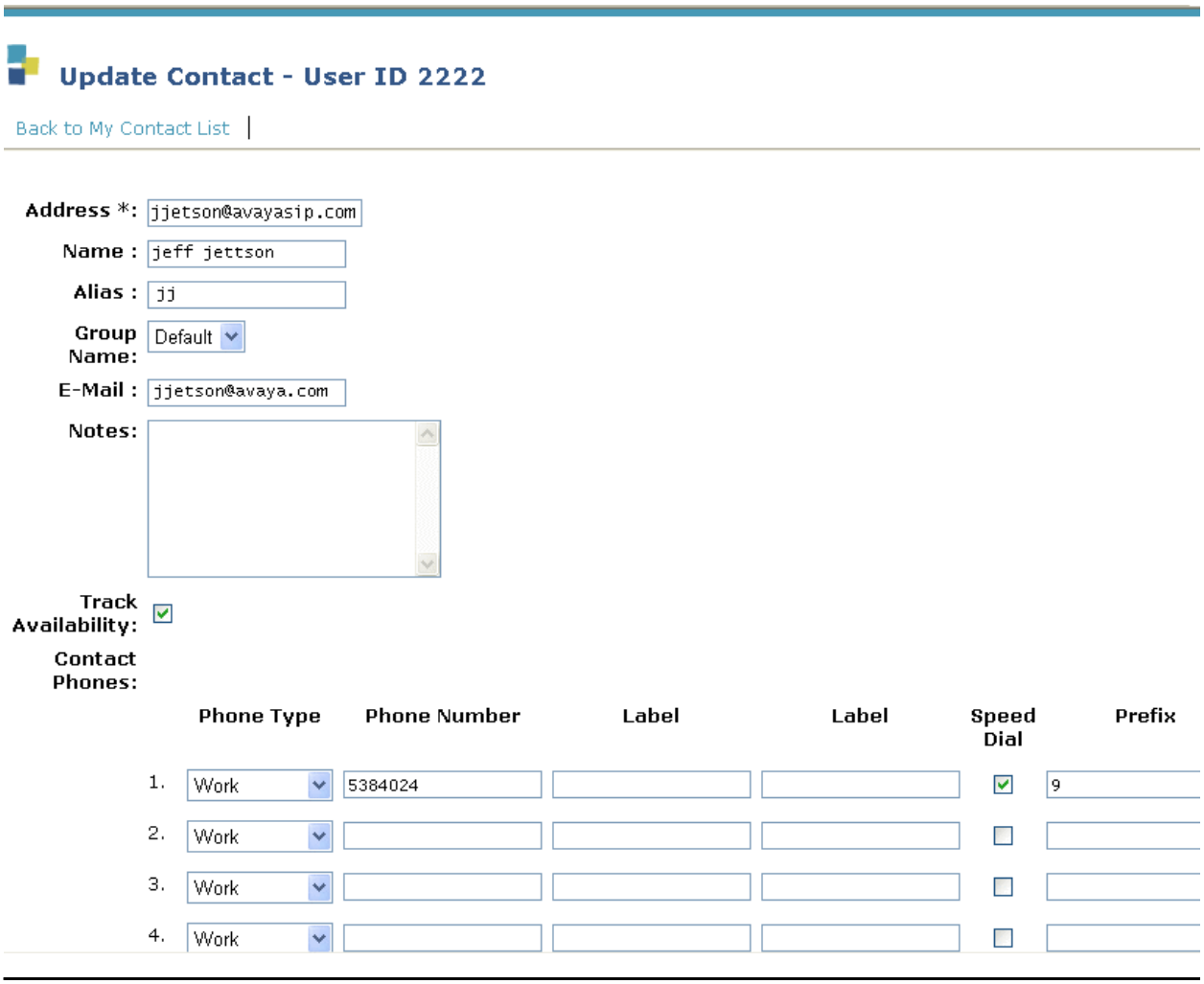
Select **Update Contact** to make changes.

Select **Delete Contact** to remove this contact's information from access by the user.

Update Contact screen

Change the contact information for the end user's contact with this screen. See the Add Contact screen on page 191 for information on field descriptions.

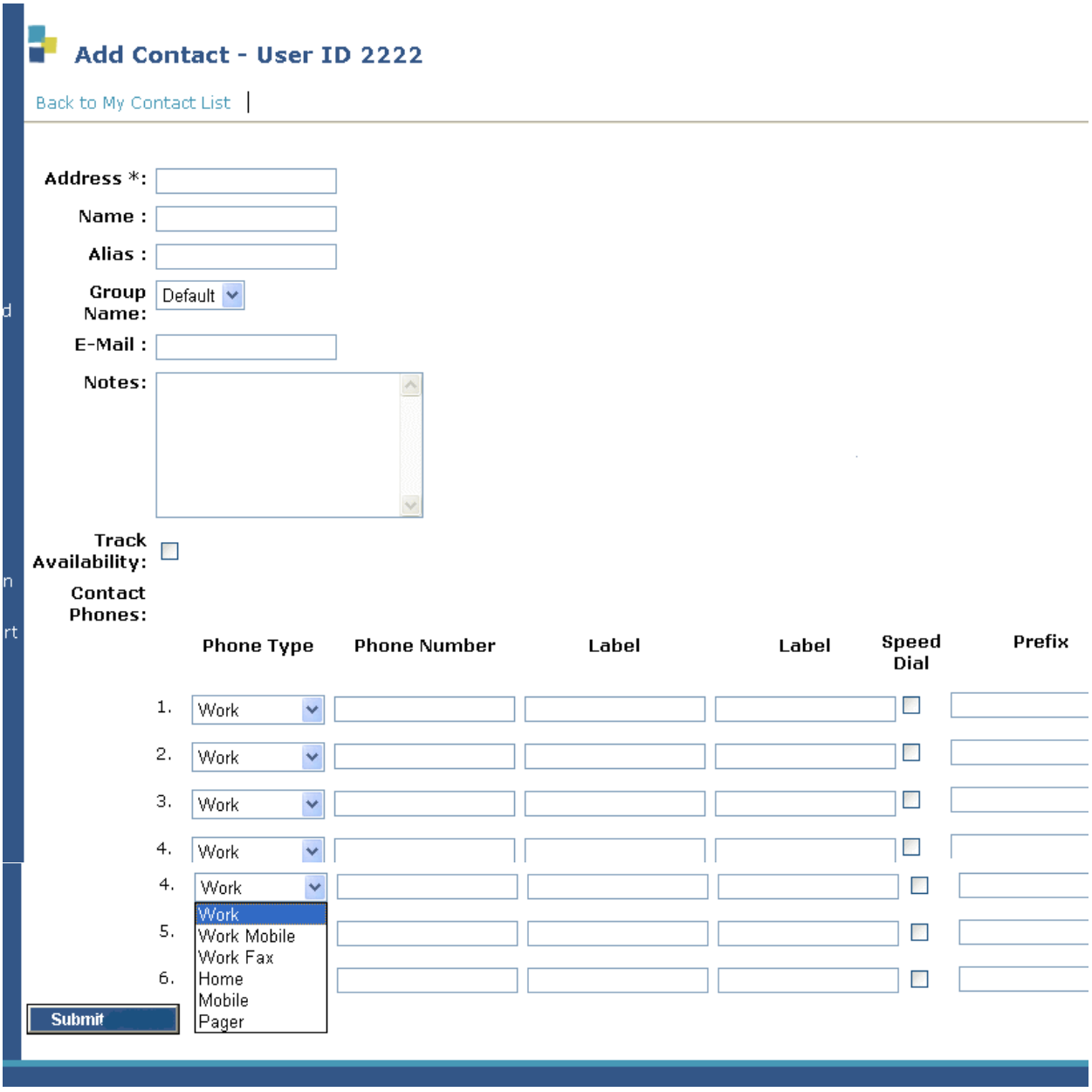
Figure 30: Update Contact



Add Contact screen

From the SIP PIM interface an end user builds a list of friends, e-mail addresses, web pages and so on, with whom to communicate. As an administrator, with this screen, you may add a contact for the end user, with a group affiliation, and speed dial numbers.

Figure 31: Add Contact screen



Add Contact and Update Contact screen field descriptions

Address

(Required) On this screen, the Address field must contain the SIP contact address of the contact in this field, that is, the user's handle on the SIP domain

Name

This is the name of as many as 64 UTF-8 characters associated with this User ID and Handle in the user database. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

The name will be assigned to the speed dial button for this contact. In Japanese, this name string uses Kanji characters. (Contrast this with Alias).

Alias

Displays the optional alias name of as many as 32 UTF-8 characters associated with this contact in the user database. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

In Japanese, this alias string is in Kana characters, and it is designed to help with contact sorting. (Contrast this with Name).

Group Name

A valid name for the group with which the contact has been associated, as a selectable link. This field may contain a maximum of 32 UTF-8 characters. Select the link to view the contact's details screen for this Group.

Tip:

If the contact list is lengthy, use your web browser's "Find in This Page" function to search the page for a particular entry.

You may select a contact to View or Delete using the radio button to the left of the name and/or handle. After you choose a contact, select the "View" button to display the Contact Details screen, or select the "Delete" button to display a warning message for you to confirm the deletion from the contact list.

Note:

Deleting a user contact from the contact list does not affect the associated provisioned user's information in the user database.

E-mail

Enter a string in this field as the e-mail address associated with this contact. It may contain as many as 256 ASCII characters. When displayed in the read-only fields on the Contact Details screen on page 189, this becomes a selectable **mailto:** link on the web page.

Notes

Enter any informational notation to be associated with this contact in this field. It is free-form text, and may contain as many as 1,024 UTF-8 characters. You can input Shift_JIS (SJIS) as well. Whether the user's browser sends UTF-8 or SJIS is dependent upon your browser's language setting.

Track Availability

Check the box if the end users wants to watch for this contact's presence in the system, using a device like SIP Softphone. End users with devices that recognize this optional parameter then will be able to watch this contact's presence and availability in the system.

Contact Phones

This group of fields lists up to six ways for a user to reach a contact.

- **Phone Type—**The drop-down menu for this field provides identification for the rest of the information in the row.
- **Phone Number—**SIP contact address, e-mail, web page, or telephone number for this contact.
- **Label / Label—**a short description of the contact, perhaps a server or type of contact.
- **Speed Dial—**check this box to let the end user reach the contact with speed dial. The first contact is speed dial number 1, the second is number 2, and so on. Speed dial is a soft button on a SIP phone
- **Prefix—**any outward dialing prefix, comma, or other sequence the end user may need to dial before they dial the phone number.

Add Contact screen command

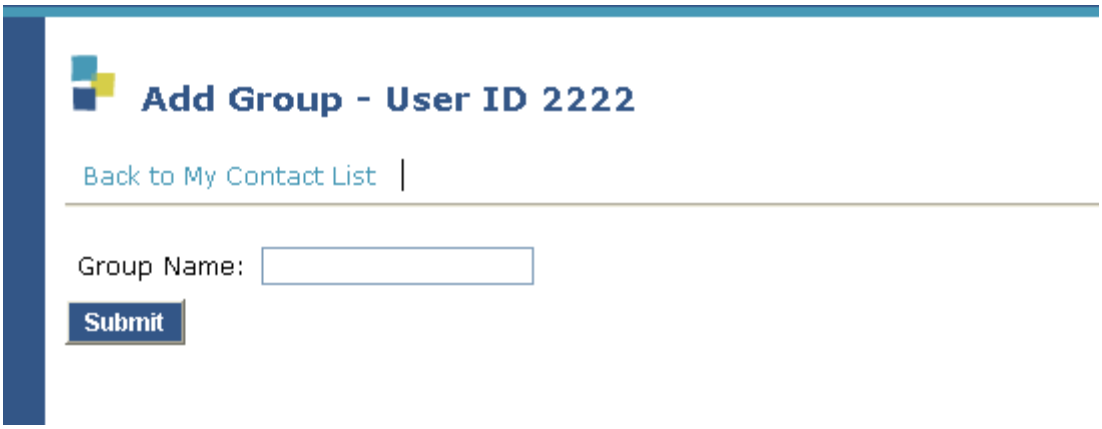
Add

Record this contact's information and it's association with a user to the database.

Add Group screen

An end user has contacts recorded that can be on speed dial. Part of the information captured about a contact is their membership in a group, for example, Test, Development, Management, or Documentation. Define groups here. Setting up a group provides a way of labeling and organizing several contacts.

Figure 32: Add Group screen



Add Group screen field descriptions

Group Name

Enter a name of as many as 32 UTF-8 characters in length for a new group for user contacts that you would like to create. You can input Shift_JIS (AKA SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon your language setting.

This is a logical name for organizational purposes, not a list name for addressing purposes via SIP contact Uniform Resource Identifiers (URIs).

Add Group screen command

Submit

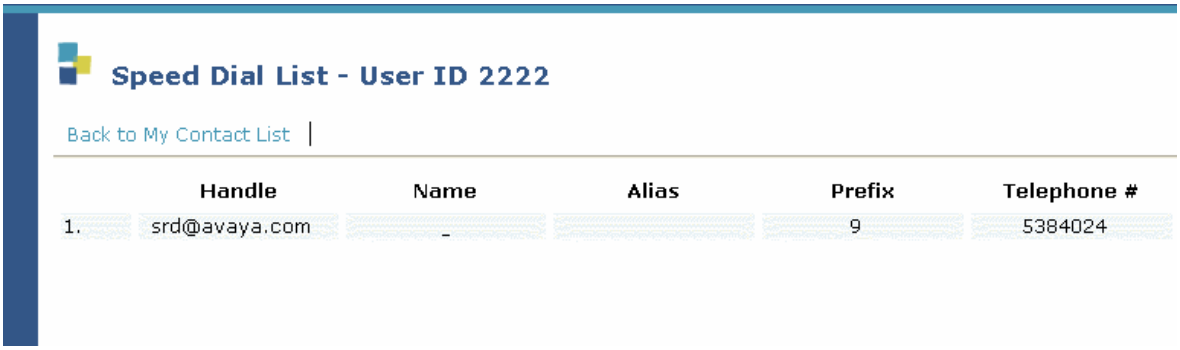
Record the new group in the database.

Speed Dial List screen

This screen is view only. It reflects the settings made in Contact Details screen on page 189. You can quickly see what is assigned to speed dial 1, speed dial 2, and so on.

To make changes to the speed dial information of a contact, use the Update Contact screen on page 190.

Figure 33: Speed Dial List screen



Handle

(Read Only) This is a valid name or User ID for the contact. Selecting this link displays the detailed user contact information for the contact this user communicates with. Handles must be unique contact URIs within the SES system domain, but contacts may have multiple valid handles.

Note:

The SES system automatically appends the *systemdomain.com* portion of the handle. This portion of the handle should not be entered as part of the handle field when adding or updating a handle.

Name

This is the name of as many as 64 UTF-8 characters associated with this User ID and Handle in the user database. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

The name will be assigned to the speed dial button for this contact. In Japanese, this name string uses Kanji characters. (Contrast this with Alias).

Alias

Displays the optional alias name of as many as 32 UTF-8 characters associated with this contact in the user database. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

In Japanese, this alias string is in Kana characters, and it is designed to help with contact sorting. (Contrast this with Name).

Prefix

(Read Only) Lists the optional prefix digits associated with this user's extension (**Telephone #**) in the user database. An example of a prefix would be an AAR or ARS dial access code of 0-4 digits. You also may leave this field blank if no such prefix code applies to this user contact.

Telephone

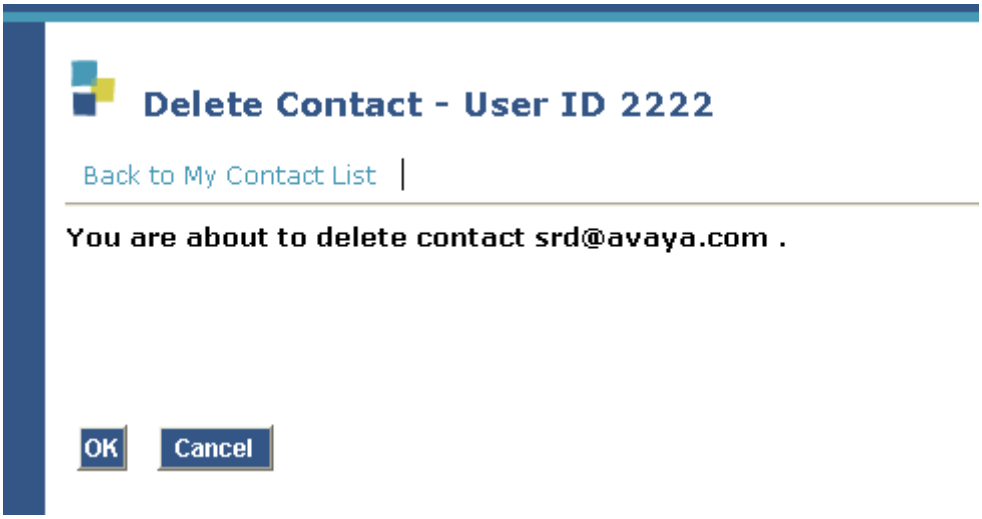
(Read Only) Lists a phone number or valid SIP user address, for example, contact Uniform Resource Identifiers (URIs) beginning with **sip:** or **sips:** and associated with this handle in the contact database. This field may contain a maximum of 256 ASCII characters.

Select **Handle** to view the associated user's detailed contact information.

Delete Contact screen

Certainly the user may want to delete infrequently used contacts over time. Deleting a contact will adjust the speed dial order. Deleting a contact does not delete the group the contact may be part of.

Figure 34: Delete Contact screen



Select OK to remove the contact from the database and remove the association from the end user.

Select Cancel if you change your mind about the delete. See the example for the Confirm Delete User screen field descriptions on page 252.

Group Details screen

If a contact can be classified with a certain group, view and delete group members here.

Figure 35: Group Detail Screen

Group Details screen field descriptions

Handle

This is a valid name or User ID for the contact. Selecting this link displays the detailed user contact information for the contact this user communicates with. Handles must be unique contact URIs within the SES system domain, but contacts may have multiple valid handles.

Note:

The SES system automatically appends the *systemdomain.com* portion of the handle. This portion of the handle should not be entered as part of the handle field when adding or updating a handle.

After viewing the details of this group, select the **Add Contact** link to go to the Add Host screen on page 165 and associate a contact with this group in your list of user contacts. Select the **Delete Group** link to go the Delete Group screen on page 201 and delete this group name from your contact list. Select the **Update Group** link to go to the Update Group screen on page 203 and change the name of this group in your user contact list.

Name

This is the name of as many as 64 UTF-8 characters associated with this User ID and Handle in the user database. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

The name will be assigned to the speed dial button for this contact. In Japanese, this name string uses Kanji characters. (Contrast this with Alias).

Alias

Displays the optional alias name of as many as 32 UTF-8 characters associated with this contact in the user database. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

In Japanese, this alias string is in Kana characters, and it is designed to help with contact sorting. (Contrast this with Name).

Telephone #1 and Telephone #2

Lists a phone number or valid SIP user address, for example, contact Uniform Resource Identifiers (URIs) beginning with **sip:** or **sips:** and associated with this handle in the contact database. This field may contain a maximum of 256 ASCII characters.

Group Details screen commands

Back to My Contact List

Select this link to return to the My Contact List.

Add Contact

Select this to display the Add Contact screen on page 191 to add another contact to the group selected.

Delete Group

Select OK to delete the group from the database. Select Cancel if you change your mind about deleting the group. See the example for the Confirm Delete User screen on page 252.

Deleting a group does not remove the contacts in the group from use. The contacts automatically become members of the default group.

Update Group

Select this to display the Update Group screen on page 203 to change the group's name.

View

Select a contact for the user and click View to show a view-only screen of the contact's details.

Delete

Delete this contact from this particular group.

This command does not delete this contact from any other groups to which it belongs.

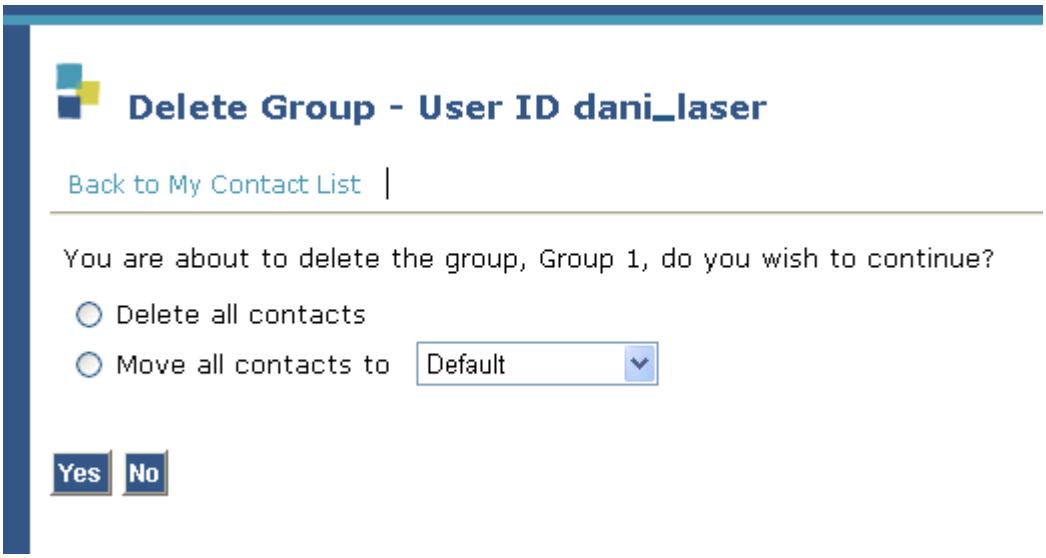
If a group is empty, View and Delete operate on the group, not members of the group. If a group is not empty, if it has members, View and Delete operate on the members and show them in the group or delete them from the group. **Delete** does not delete a group member from the database.

Delete Group screen

Deleting a group generates the following results:

- Delete the group and all its members.
- Move the members to another group and then remove the original group.

Figure 36: Delete Group screen



Delete Group screen field descriptions

Delete all contacts

Select this radio button to remove the members from the group but keep the group itself. The contacts are not deleted from the system.

Move all contacts

Select this to move all the group's members to another group. The original group is deleted.

Delete Group screen commands

Back to My Contact List

Select this link to return to the My Contact List screen.

Yes

Go ahead and invoke your selections.

No

Cancel the selections on the screen and do nothing. The system displays the My Contacts screen.

Update Group screen

If the name of the group contacts are categorized in changes, modify the group name here. For example, you might want to change the group name Test Team to User Experience Testing. All contacts associated with the first group name now are associated with the new group name.

Figure 37: Update Group Screen

Update Group screen field descriptions

Old Group Name

Displays the name of the existing group that you are about to change.

Group Name

(Required) Enter a new name for the existing group, of as many as 32 UTF-8 characters in length. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

In Japanese, this alias string is in Kana characters, and it is designed to help with contact sorting. (Contrast this with name).

When finished entering data, select **Submit** to rename the group in your contact list.

Update Group screen commands

Back to My Contact List

Select this link to return to the Contact List

Submit Update

Select this to apply the change to the database.

Devices Screen menu

Figure 38: Devices screen allows the users of certain supported SIP devices to view, change, and reload certain configuration settings. Note that the example screens shown in this section apply exclusively to the new Toshiba SIP Business Telephone SP-1020A in this release of Avaya SIP Personal Information Manager (PIM), and they do not apply to the other SIP-enabled client devices offered by Avaya, like the Avaya 4600-series IP Telephones, Avaya Softphone Release 5.x or Avaya SIP Softphone Release 2.x.

Figure 38: Devices screen

Devices screen description

Terminal Information

This screen shows the attributes of a user's phone (terminal), such as vendor, software version, and MAC address. This screen is view only for the administrator.

One Touch Dial List

Use this screen to view or edit the applicable One Touch Dial List entries for the buttons on your telephone, if any, which have been administered using the screens for the station's auto-dial feature in Avaya Communication Manager software running on a media server.

Ringer Settings

This screen lets you turn the ringer on and off for the user, and shows information about the phone’s bridged appearance.

Tones and Volumes Settings

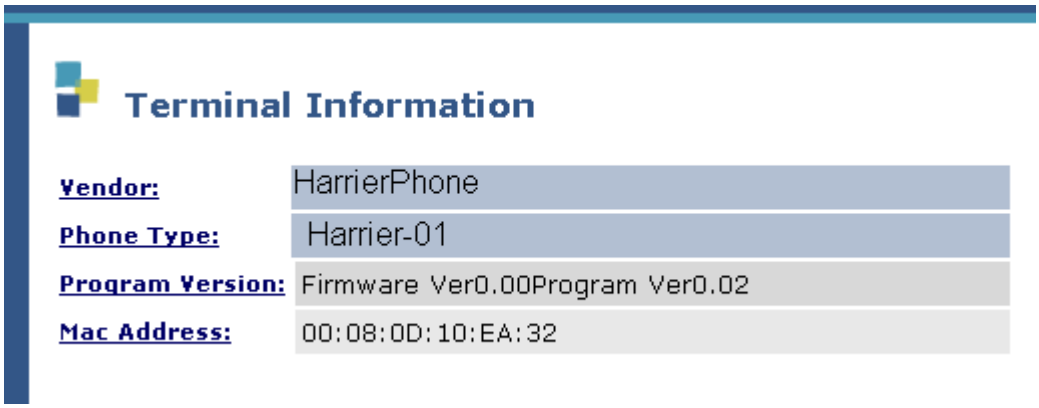
This screen shows how a user has set the telephone’s tones and volume. This screen is view only for the administrator.

Terminal Information screen

This screen is also available on the web page viewed by the user, the SIP Personal Information Manager pages. For you to view this screen, the end user must have a compatible device.

This screen is view only for the administrator.

Figure 39: Terminal Information screen



Terminal Information screen field descriptions

Vendor

This label indicates the name of the manufacturer and station type for certain SIP phones. For release R3.0 of SIP Personal Information Manager (PIM), this example applies to the Toshiba SIP Business Phone SP-1020A. If the information is not provided by the device, a message to that effect will be displayed in this area.

Phone Type

The model number of the manufacturer's phone.

Program Version

The version of software this phone uses.

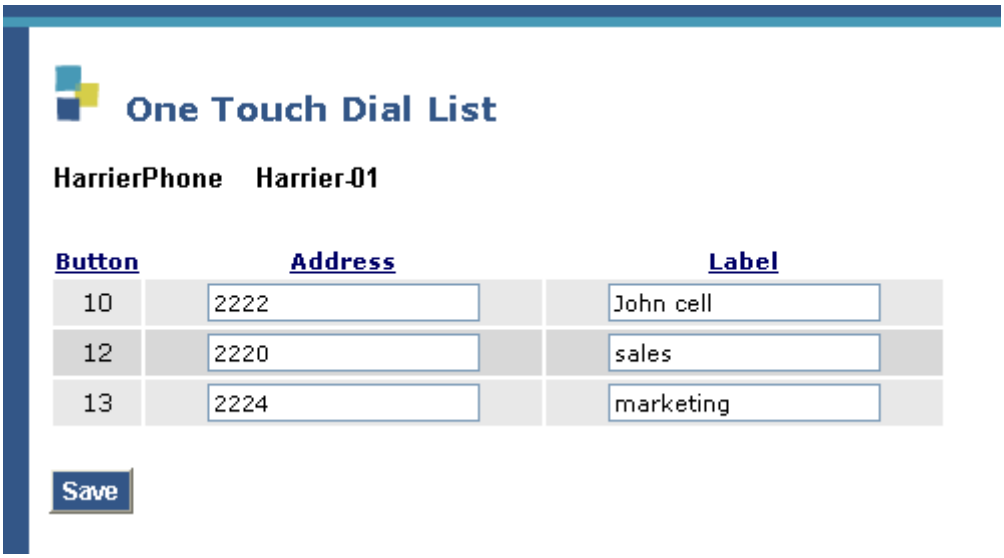
MAC Address

The media access control address, that uniquely identifies this device on the network.

One Touch Dial List screen

This screen is also available on the web page viewed by the user, the SIP Personal Information Manager pages. For you to view this screen, the end user must have a compatible device.

Figure 40: One Touch Dial List screen



One Touch Dial List screen field descriptions

Button

The number designating the button which is assigned to this auto-dial list entry in Avaya Communication Manager running on the media server. The maximum button number is 66.

Address

May be blank, in which case SIP contact Uniform Resource Identifiers (URIs) for the auto-dial list entry may be entered here, or it may display the non-blank auto-dial list entry or entries made in Avaya Communication Manager running on the media server for the associated button. In the latter case, if the entry is edited in this SIP PIM web interface, any changes made to these entries here will ***not*** be reflected in Communication Manager on the media server(s). The maximum length of any Address field entry is 256 ASCII characters.

Label

May be blank, in which case a label for the auto-dial entry may be entered here, or it may display (read-only) the non-blank auto-dial entry label made in Avaya Communication Manager running on the media server for the associated button. In the latter case, the entry may not be edited here. The maximum length of any Label field entry is 20 UTF-8 characters. Note that UTF-8 characters can include ASCII, Kanji and Kana characters. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

In Japanese, this alias string is in Kana characters, and it is designed to help with contact sorting. (Contrast this with name).

Note:

The Toshiba SIP Business Telephone SP-1020A does not display half-width, Han Kaku Kana characters.

One Touch Dial List screen commands

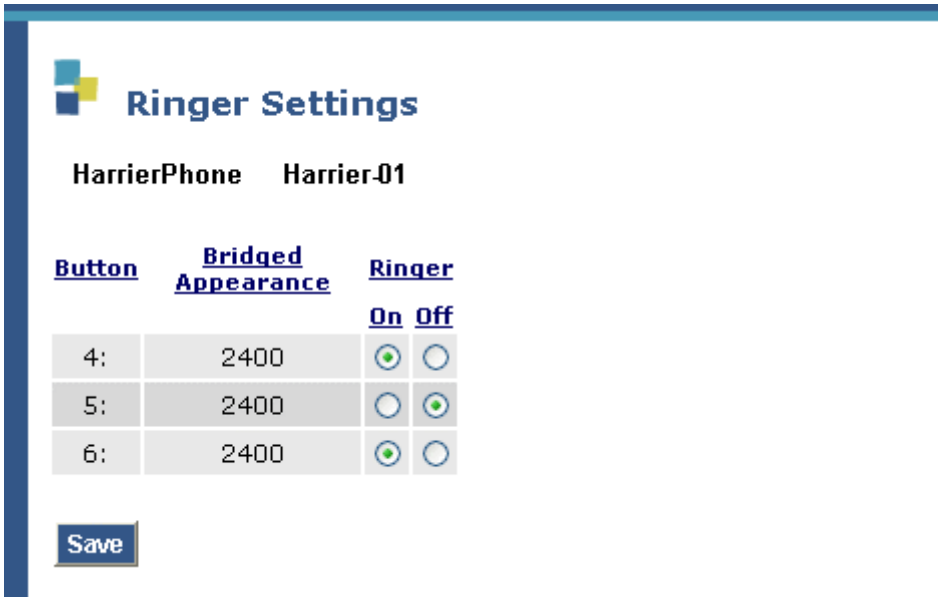
Save

Commit the one touch dial information to the database.

Ringer Settings screen

This screen lets you turn the ringer on and off for the user, and shows information about the phone's bridged appearance. This screen is also available on the web page viewed by the user, the SIP Personal Information Manager pages. For you to view this screen, the end user must have a compatible device.

Figure 41: Ringer Settings screen



Ringer Settings screen field description

Button

(Read only) Displays one or more number(s) designating the bridged appearance button(s) on your phone for which you may turn the ringer on or off (and independent of and not reflecting the OPS settings for the station in Avaya Communication Manager running on a media server).

Setting the ringer settings is for the station's bridge appearance buttons. This is not related to ringer settings configured on Communications Manager.

Bridged Appearance

(Read only) Lists the media server extension associated with this phone button in the user database. This field may contain a maximum of 256 alphanumeric characters.

Ringer ON/OFF

If the ringer of any available button is set to off, you may select the radio button under On to enable its ringer. Likewise, if it is set to On, you may select the button under Off to disable it.

Ringer Settings screen command

Save

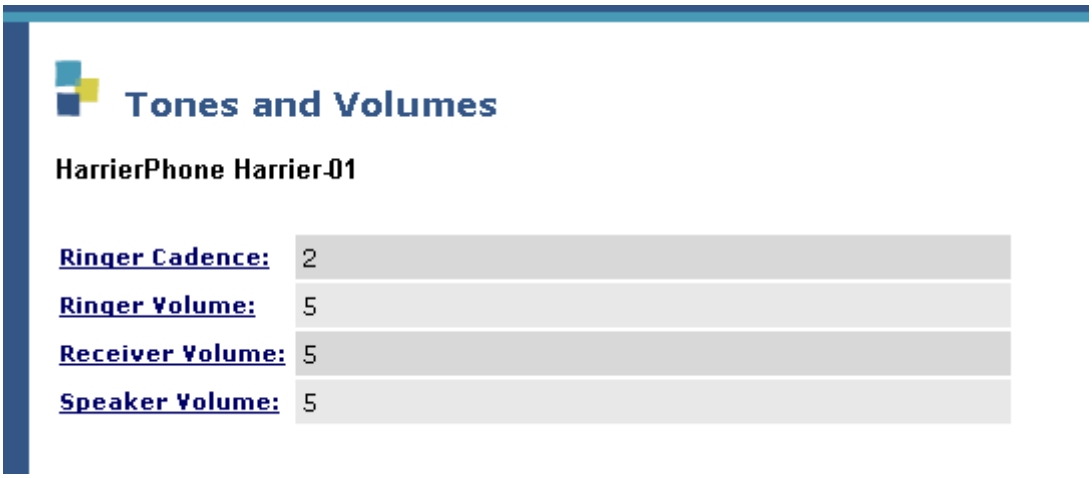
Commit the ringer settings to the database.

Tone and Volume Settings screen

This screen is view only for the administrator, and provides a list of how the tones, volumes and speed of the user's telephone device were set by the user.

This screen is also available on the web page viewed by the user, the SIP Personal Information Manager pages. For you to view this screen, the end user must have a compatible device.

Figure 42: View Tones and Volumes screen



Ringer Cadence

(Read Only) Displays the default Ringer Cadence (default is 2) for your device administered for end users in the database. This number represents the speed of the telephone's ringing (1 through 3).

Ringer Volume

(Read Only) Displays the default Ringer Volume (default is 5) for a device administered for end users in the database. This number represents how loudly the telephone will ring. The range is 1 through 10.

Receiver Volume

(Read Only) Displays the default Receiver Volume (default is 5) for your device administered for end users in the database. This number represents the loudness of your handset (1 through 10).

Speaker Volume

(Read Only) Displays the default Speaker Volume (default is 5) for your device administered for end users in the database. This number represents the loudness of your speakerphone (1 through 10).

Extensions task

This section describes administering a specific user's extension. For example, you can associate an extension with a user, remove an extension from a user, or free an extension for use by any other user with this screen series.

If you want to deal with extensions on the Communication Manager media server, perhaps to make more extensions available, see the menu for the Media Server screens on page 295.

Figure 43: List Media Server Extensions screen

List Media Server Extensions screen field descriptions

Extension

The numeric telephone extension in the database.

This is the extension for the user named to the right.

User

This is the User ID. An identifier of at least three alphanumeric characters in length, used to authenticate a user to the SES system. Each user has one unique user ID, and, the User ID is the same as the user's handle. A User ID may be a name or an ID number.

Media Server

The name of the media server this user is registered on.

Host

This is the name of the home server for this user.

List Media Server Extensions screen commands

Free

This command removes an extension from the selected user, but keeps it available on the media server. Select this to render an OK Cancel screen. See the example for the Confirm Delete User screen on page 252.

Edit User

For the convenience of the administrator, this selection lets you display this user as the only user in the list. Usage is described in the List Users screen on page 180. Pick a task from the drop-down list.

Delete

This command deletes an extension from the user. The user remains, but has no extension.

Select this to render an OK Cancel screen. See the example for theConfirm Delete User screen on page 252.

Handles task

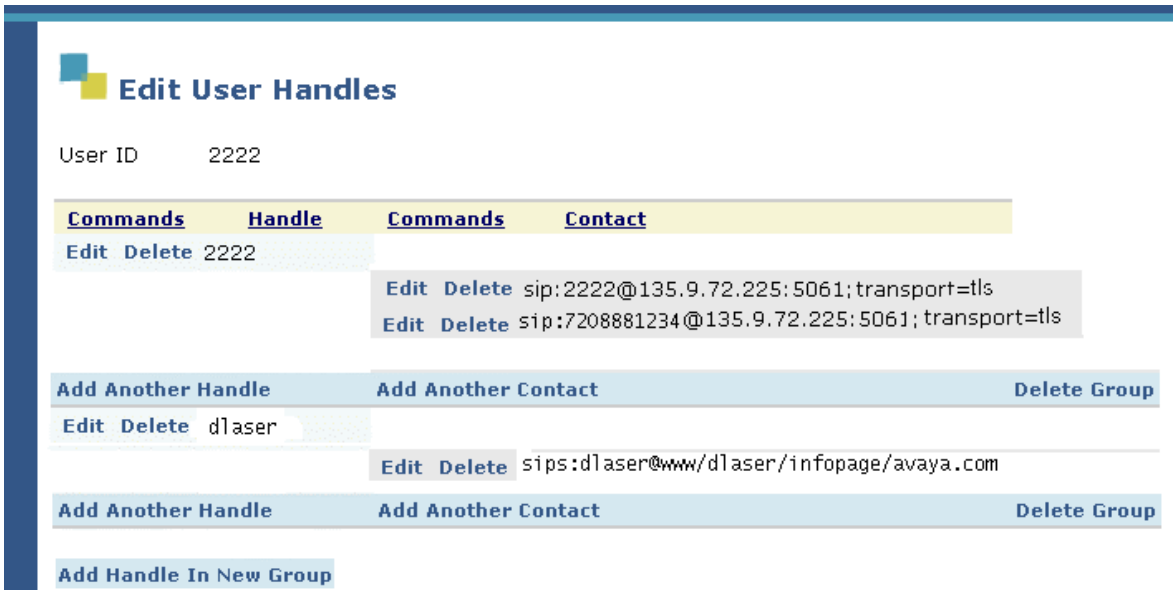
One way to get to this screen is to select List Users, find the user you want, click the check box. From the task drop-down list select **Handles**. Click **Submit**.

The Handles task concerns how the end user wants to be contacted.

Handles identify user's on the SES system, and, provide two ways to contact the user. If the user has a second handle, that handle may resolve to an email address and a web page.

Handles must be unique across the system.

Figure 44: Edit User Handles screen



Do not use the handles listed below for a user. They are reserved for system and administrator use:

- event-server
- cm-resubscribe
- confsvr
- presenceserver

In addition:

- Handles longer than 256 characters are truncated.
- If any of the preceding transformations produce handles already present, then they are dropped.
- No user handle may start with an underscore.

- All handles must be entered in lower case.
- All handles must be unique
- All handles must be alphanumeric and may contain a period, '-' (dash) or '_' (underscore)
- All handles must be between 3 and 16 ASCII characters.

Edit User Handles screen field descriptions

User ID

(Read only) An identifier of at least three alphanumeric characters in length, used to authenticate a user to the SES system. Each user has one unique user ID, and, the User ID is the same as the user's handle. A User ID may be a name or an ID number.

Handle

A handle identifies the user on the SES system. The user's handle must be the same as their user ID. Selecting the link displays the detailed user contact information for the associated user. Handles must be unique, contact Uniform Resource Identifiers (URI) within the SES system domain. Users may have multiple handles to accommodate more that two personal points of contact to the user.

Note:

The SES system automatically appends the `@sip_domain.com` portion of the handle. Do not type this portion of the handle when adding or updating this end user on other screens.

Contact

In this screen, the information in the Contact column is the SIP address of the user, which is created based on the user's telephone extension and the IP address of the media server this user is assigned to.

In the example in Figure 44, The User ID, 2222, has two handles: **2222** and **dlaser**. Contacts for 2222 show the user's media server extension and a cell phone number. Contacts for dlaser show a web page where the user posts the latest information regarding work.

Edit User Handles screen commands

Edit (Handle)

Go to the Edit Handle detail screen on page 219 for that user's handle for the associated user Contact.

Delete (Handle)

Display the **Confirm Delete Handle** screen for that user's handle, or to display the **Confirm Delete Contact** screen for that user's contact entry. The handle that has no Delete command next to it is the primary handle

Add Another Handle

You may select **Add Another Handle** to go to the Add Handle screen on page 223.

Edit (Contact)

Go to the Edit Host Contact screen on page 221 for the associated user Contact.

Delete (Contact)

Display the **Confirm Delete Contact** screen for that user's contact entry.

Add Another Contact

Select this link to add another contact for the user with the Add Host Contact screen on page 225.

Add Handle in New Group

A group is a set of handles that resolves to a set of contacts.

Select **Add Handle In New Group** to go to the Add Handle in a New Group screen on page 228. There, you can add a handle to a newly created group.

Delete Group

Select **Delete Group** to display the **Confirm Delete Group** screen. When viewing the confirmation screen, select to delete the group and all its members, or to delete only the group association of the members, and leave the member contacts available.

Edit Handle detail screen

Change the users handle at any time with this screen.

Figure 45: Edit Handle, Detail screen

Edit Handle detail screen field description

User ID

(Read Only) An identifier of at least three alphanumeric characters in length, used to authenticate a user to the SES system. Each user has one unique user ID, and, the User ID is the same as the user's handle. A User ID may be a name or an ID number.

Domain

The domain name of the home server this user is assigned to.

Handle

(Required) A handle identifies the user on the SES system. The user's handle must be the same as their user ID. Selecting the link displays the detailed user contact information for the associated user. Handles must be unique, contact Uniform Resource Identifiers (URI) within the SES system domain. Users may have multiple handles to accommodate more that two personal points of contact to the user.

Note:

The SES system automatically appends the `@sip_domain.com` portion of the handle. Do not type this portion of the handle when adding or updating this end user on other screens.

Do not use the handles listed below for a user. They are reserved for system and administrator use:

- event-server
- cm-resubscribe
- confsvr
- presenceserver

In addition:

- Handles longer than 256 characters are truncated.
- If any of the preceding transformations produce handles already present, then they are dropped.
- No user handle may start with an underscore.
- All handles must be entered in lower case.
- All handles must be unique
- All handles must be alphanumeric and may contain a period, '-' (dash) or '_' (underscore)
- All handles must be between 3 and 16 ASCII characters.

Edit Handle detail screen command

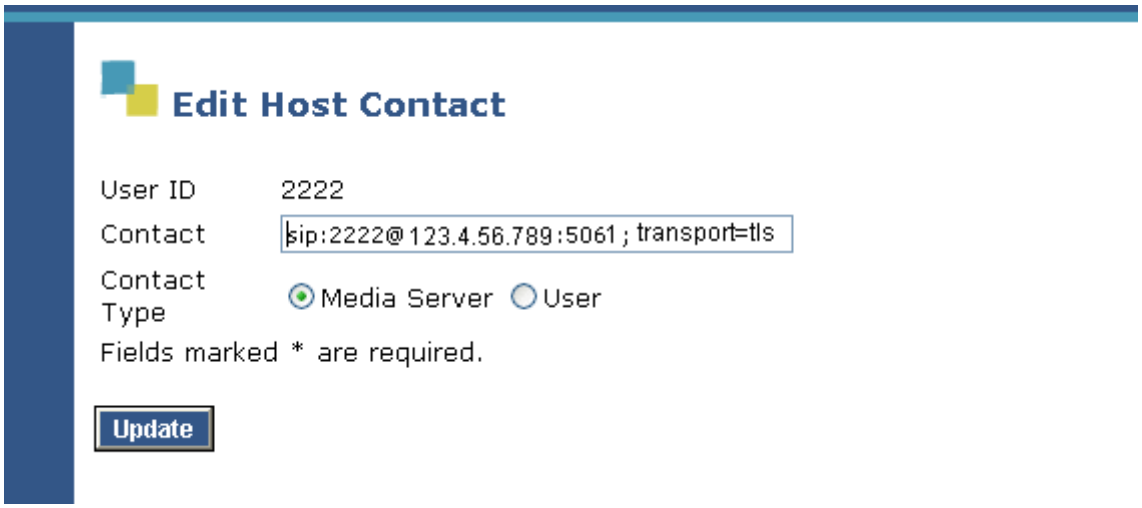
Update

Select Update to commit the information to the database.

Edit Host Contact screen

This screen lets you change a specific user's host contact to a different media server.

Figure 46: Edit Host Contact screen



Edit Host Contact screen field descriptions

User ID

(Read only) The user ID for whom you want to name a new host.

Contact

In this screen, the Contact field identifies either a media server, or any other server or device.

For this screen there are two types of contact information, Media Server and User.

The **Media Server contact type** is for all handles that should be resolved to contacts that are routed directly to a media server. This only includes handles that are also extensions, because media servers only recognize extensions, not user handles.

If you select the Media Server contact type, the entered Contact pattern should be a contact that includes a media server IP address.

If you select the Media Server contact radio button, the system is expecting that the corresponding contact is a media server contact. If you select the Media Server contact type, and the corresponding contact is *not* pattern recognized by the media server, then calls may not get routed.

The **User contact type** is used for all handles that should be resolved to contacts that are directly routed to addresses that are *not* media servers. This includes other home servers, or devices that are not connected to a media server.

If you select the User contact type, the entered Contact on the page should be a contact that is *not* a media server IP address.

If you select User contact type, and the corresponding contact is a media server, then calls may get routed to the media server but not complete.

Edit Host Contact screen commands

Media Server option

Specify that the information in the Contact field is a users primary SIP contact address that is recognizable by the media server. The call will route successfully through the media server.

User option

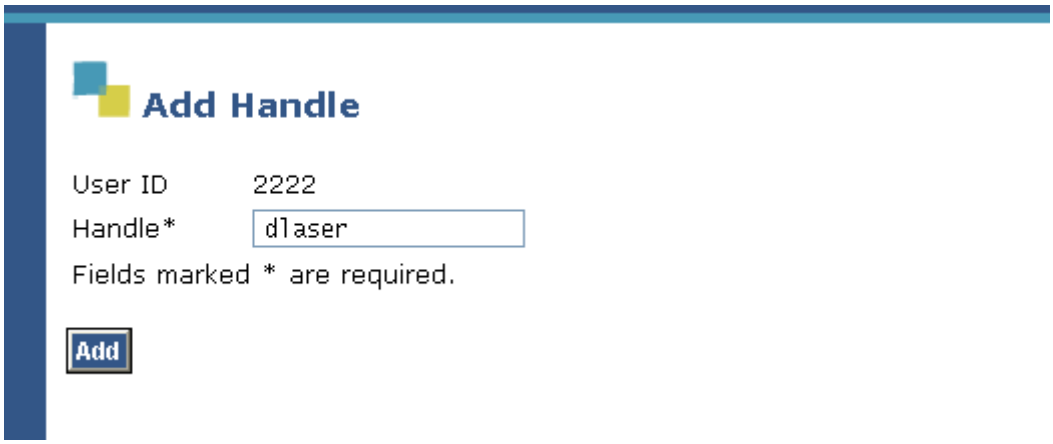
Indicate that the information in the Contact field is not a user’s primary SIP contact address, and should not be routed through the media server.

Update

Commit your changes to the database.

Add Handle screen

Figure 47: Add Handle screen



Add Another Handle screen field descriptions

User ID

(Read Only) An identifier of at least three alphanumeric characters in length, used to authenticate a user.

Handle

(Required) A handle identifies the user on the SES system. The user's handle must be the same as their user ID. Selecting the link displays the detailed user contact information for the associated user. Handles must be unique, contact Uniform Resource Identifiers (URI) within the SES system domain. Users may have multiple handles to accommodate more that two personal points of contact to the user.

Note:

The SES system automatically appends the `@sip_domain.com` portion of the handle. Do not type this portion of the handle when adding or updating this end user on other screens.

This is never the primary handle, which is defined in the Add User screen on page 237.

Do not use the handles listed below for a user. They are reserved for system and administrator use:

- event-server
- cm-resubscribe
- confsvr
- presenceserver

In addition:

- Handles longer than 256 characters are truncated.
- If any of the preceding transformations produce handles already present, then they are dropped.
- No user handle may start with an underscore.
- All handles must be entered in lower case.
- All handles must be unique
- All handles must be alphanumeric and may contain a period, '-' (dash) or '_' (underscore)
- All handles must be between 3 and 16 ASCII characters.

Add Another Handle screen command

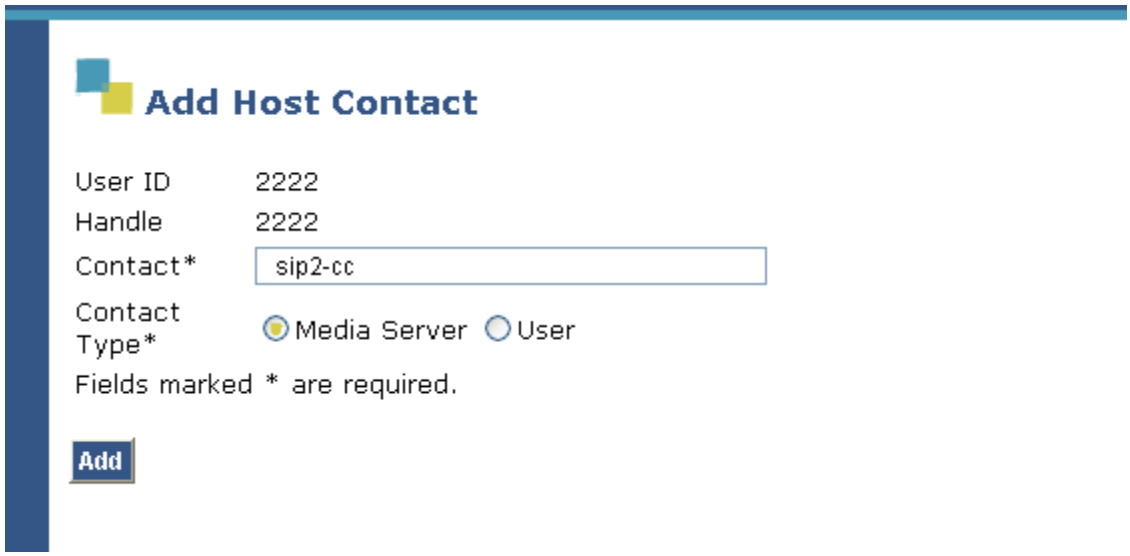
Add

Create another SIP address for this user.

Add Host Contact screen

A contact for a host, can be either a media server URI or a user URI.

Figure 48: Add Host Contact screen



Add Host Contact screen field descriptions

User ID

(Read only) An identifier of at least three alphanumeric characters in length, used to authenticate a user.

Handle

(Read only) A handle identifies the user on the SES system. The user's handle must be the same as their user ID. Selecting the link displays the detailed user contact information for the associated user. Handles must be unique, contact Uniform Resource Identifiers (URI) within the SES system domain. Users may have multiple handles to accommodate more that two personal points of contact to the user.

Note:

The SES system automatically appends the `@sip_domain.com` portion of the handle. Do not type this portion of the handle when adding or updating this end user on other screens.

Contact and Contact Type

(Required) In this screen, the Contact field identifies either a media server, or any other server or device.

For this screen there are two types of contact information, Media Server and User.

The **Media Server contact type** is for all handles that should be resolved to contacts that are routed directly to a media server. This only includes handles that are also extensions, because media servers only recognize extensions, not user handles.

If you select the Media Server contact type, the entered Contact pattern should be a contact that includes a media server IP address.

If you select the Media Server contact radio button, the system is expecting that the corresponding contact is a media server contact. If you select the Media Server contact type, and the corresponding contact is *not* pattern recognized by the media server, then calls may not get routed.

The **User contact type** is used for all handles that should be resolved to contacts that are directly routed to addresses that are *not* media servers. This includes other home servers, or devices that are not connected to a media server.

If you select the User contact type, the entered Contact on the page should be a contact that is *not* a media server IP address.

If you select User contact type, and the corresponding contact is a media server, then calls may get routed to the media server but not complete.

Add Host Contact screen commands

Media Server option

Specify that the information in the Contact field is a user's primary SIP contact address that is recognizable by the media server. The call will route successfully through the media server.

User option

Indicate that the information in the Contact field is not a user's primary SIP contact address, and should not be routed through the media server.

Add

Confirm to add the new host contact you have set up.

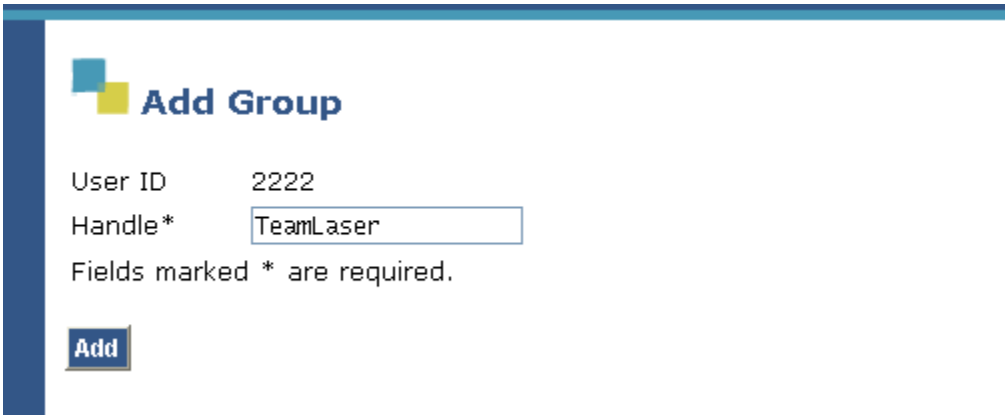
Add Handle in a New Group screen

Add Handle in **New Group** renders a New Group screen, specifically for groups of users that resolve to the same Contact.

A group is a set of handles that resolves to a set of contacts.

Even though the screen title says Add Group, you are adding the handle in the required field to the group you selected previously.

Figure 49: Add Group screen



Add Group screen field descriptions

User ID

(Read only) An identifier of at least three alphanumeric characters in length, used to authenticate.

Handle

(Required) In this screen, enter a handle of any end user to include them in this group.

Do not use the handles listed below for a user. They are reserved for system and administrator use:

- event-server
- cm-resubscribe
- confsvr
- presenceserver

In addition:

- Handles longer than 256 characters are truncated.
- If any of the preceding transformations produce handles already present, then they are dropped.
- No user handle may start with an underscore.
- All handles must be entered in lower case.
- All handles must be unique
- All handles must be alphanumeric and may contain a period, '-' (dash) or '_' (underscore)
- All handles must be between 3 and 16 ASCII characters.

Add Group screen commands

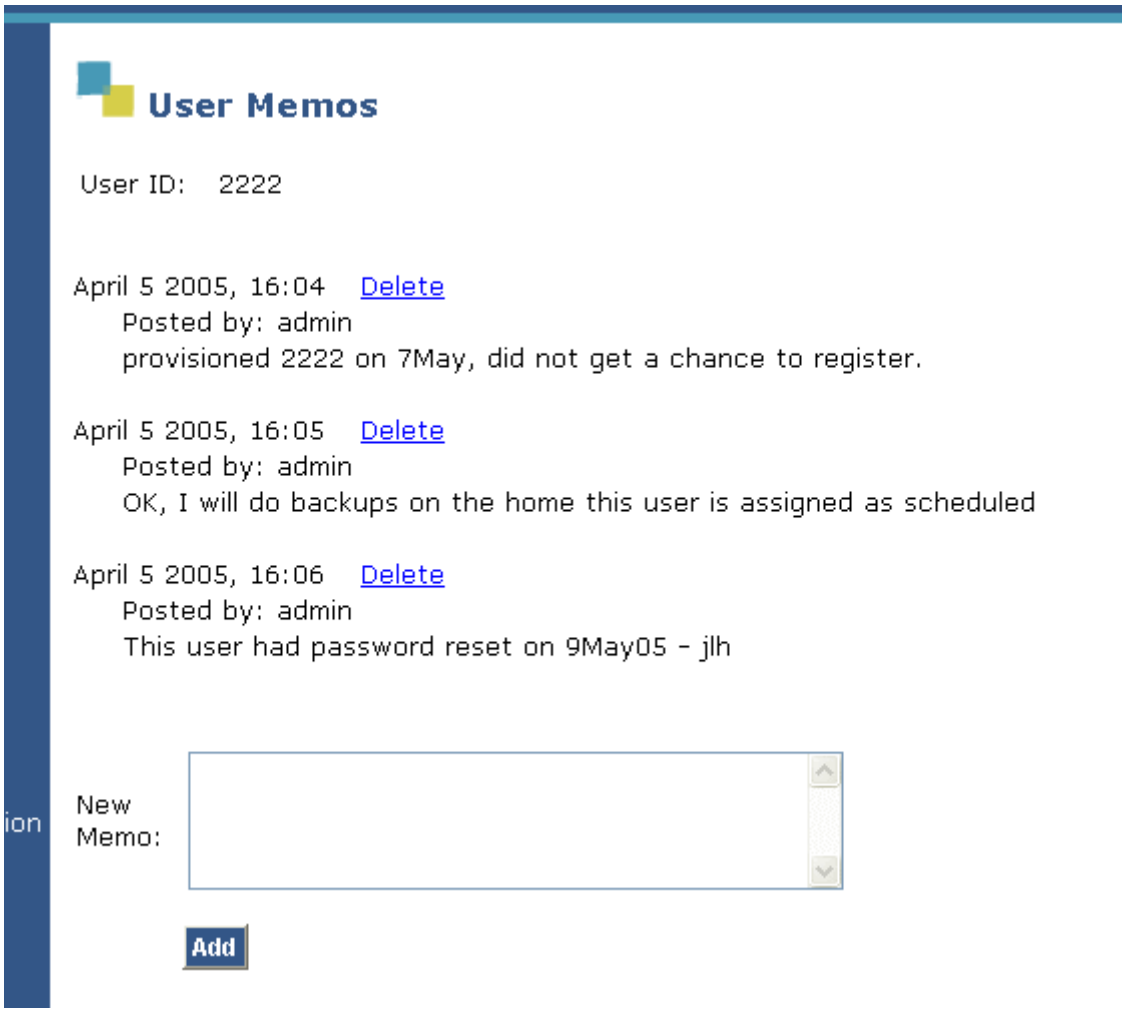
Add

Add the specified new group.

User Memos screen

This screen lets administrators write memos about a user. The memos are available only to another administrator looking at this screen. End users do not see this information.

Figure 50: User Memo screen



User Memo field descriptions

User ID

An identifier of at least three alphanumeric characters in length, used to authenticate a user.

List of memos

The available memos display in chronological order, most recent at the top.

Add Memo box

Write a new memo about the user inside this text box.

Delete

Remove the memo to the left.

Add Memo button

Select this button to store the memo in the area above.

Permissions screen

The Permissions page manages a user's control over presence, who they permit to see them on the system. This page has four versions, depending on the current setting, and every page allows the setting to be changed to the other type.

Figure 51: Permissions screen

Permissions screen field descriptions

Current Permissions Type

(Read Only) Note the type of Permissions that now are set for the user. The types of Permissions are **Allow All**, **Block All**, and **Contact List Only**. **Block All** is the default permission type for any user unless you specify a different type of permissions or modify the user's permissions. To modify the current Permissions type that is displayed for this user, you may use Permissions screen on page 232.

Change Permissions Type

The drop-down list provides three levels of permissions:

- Allow All—Select **Allow All** if you want all administered SIP users to be able to watch this user's presence and availability in the system, using any presence-enabled SIP client like Avaya IP Softphone.
- Block All—Select **Block All** if you want no administered SIP users to be able to watch this user's presence and availability in the system.
- Contact List Only—Select **Contact List Only** if you want only those administered SIP users that you have added to your contact list to be able to watch this user's presence and availability in the system.

After selecting the appropriate permissions type, select the Change button to commit the entry to the user contact database.

Handle

This is a selectable link, a valid handle for the blocked or allowed caller. Selecting the link displays the detailed user contact information for the associated user. Handles must be unique contact Uniform Resource Identifiers (URI) within the SIP domain.

Note:

If entering or changing the Handle, only provide characters for the portion in front of the `@` sign. The system automatically appends the `@systemdomain.com` portion of the handle.

Permissions screen commands

Change Permissions Type

Choose from the drop-down list of user-contact permissions:

Allow All — permits all administered SIP users to note your presence in the system.

Block All — permits *no* administered SIP users to note your presence in the system.

Contact List Only — lets only those administered SIP users on the user's contact list to be able to observe your presence in the system.

Allow List/Block List

(Read Only) Lists any users for whom there are discrete entries to Allow permission or Block permission to watch this user's presence and availability on the system. If the Current Permissions Type is set to **Contact List Only**, then the Allow List/Block List does not display. Instead, you may select the link to view the members who are allowed to watch this user's presence and availability in the system. If you wish to delete the **Block** (or **Allow**) permission type entry for a specific person on the list, then select the Remove link.

Note:

If you didn't specify a domain for a user on either list, then the SIP system *domain.com* will be appended automatically to the user contact entry.

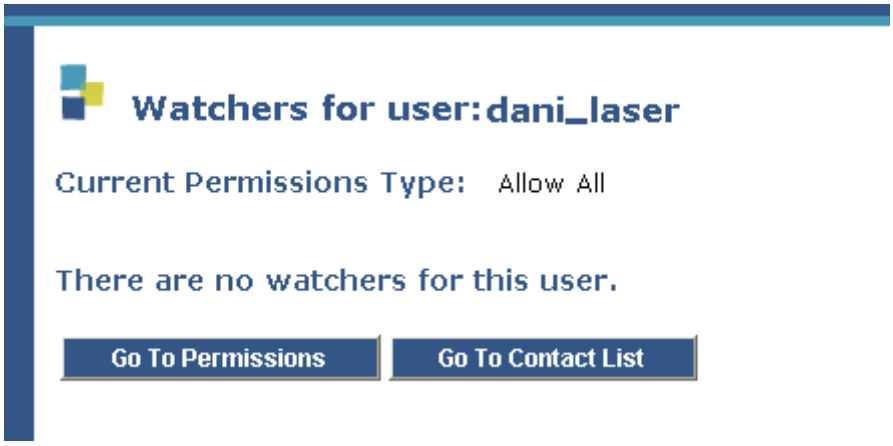
Add Entry

Use this area to add a valid user handle to one of the two permissions lists, Allow or Block. To remove a permission entry, select from the **Allow List/Block List** field.

Watchers Task

The Watchers screen quickly relays the level of watch permissions this user has set. Then, with the command buttons, you can adjust that level using either the Permissions screen or the Contacts list.

Figure 52: Watcher's screen



Watchers screen field descriptions

Current Permissions Type

Note the type of Permissions that now are set for the current user. The types of Permissions are **Allow All**, **Block All**, and **Contact List Only**. **Block All** is the default permission type for any user unless you or the user specify a different type of permission, or modify the user's permissions. To modify the current Permissions type displayed for this user, you may use **Change Permissions Type** field on the Permissions screen on page 232.

Tip:

Changing the Current Permissions Type does not interactively add or delete existing exception entries made on the Allow List/Block List. That is, if you change from Block All to Allow All, then any exceptions on the Block List remain in effect. Likewise, if you change from Allow All to Block All, then any exceptions on the Allow List remain in effect.

Contact List Members

(Read Only) This area of the screen lists members of the end user's contact list who are aware of the end user's presence, that is, who have subscribed to be updated on your presence and availability in the system. If no such users exist and are subscribed, then this field does not appear on this page.

Select the associated link to the right to **Block** a **Contact List Member** from being able to watch your presence and availability in this system.

Unknown (SIP Users)

(Read Only) Lists any SIP users not on your contact list, but provisioned in this system, and for whom you have added discrete entries to **Allow** permission to watch your presence. If no such entries have been made, this field does not appear on this page. If you wish to **Block** permission for a specific unknown SIP user from being able to watch your presence and availability in this system, then select the link to the right of the list entry. To change the default permissions for all SIP users, then select the **Go To Permissions** link and use the **Change Permissions Type** field on the Permissions screen. If you want to add any of the SIP users who are unknown to this system to your list of (known) user contacts, for example to watch their presence and availability, then you may select the **Add to Contact List** link to the right of any **Unknown** list member.

Watchers screen commands

Go to Permissions

Select this to change the current level of permissions for the user. The system displays the Permissions screen on page 232.

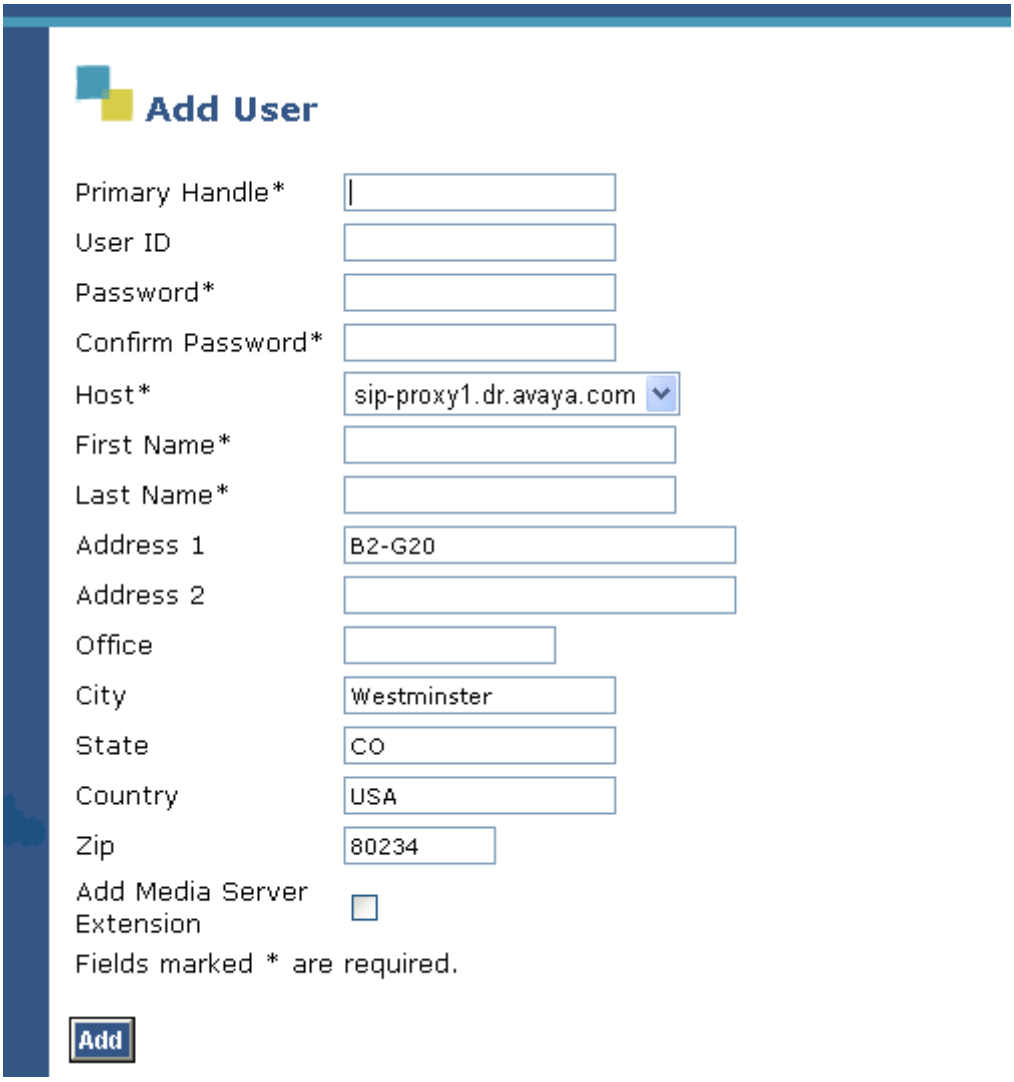
Go to Contact List

Select this to add more contacts to the users contact list. Doing so makes the permission type of Contact List Only more inclusive. See Contact List task on page 185.

Add User screen

Add users one at a time with this screen. The contents of the default user profile are used for the fields Host, Address 1, Address 2, City, Country, and ZIP. You may change those entries here for this single user. Click **Add Media Server Extension** to immediately assign a media server extension, and a SIP address based on that extension, to the added user.

Figure 53: Add User screen



The fields for user profiles now accepts UTF-8 encodings to accommodate multibyte character languages such as Japanese. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

The name will be assigned to the speed dial button for this contact. In Japanese, this name string uses Kanji characters. (Contrast this with alias).

Add User screen field descriptions

Primary Handle

(Required) A handle identifies the user on the SES system. The user's handle must be the same as their user ID. Selecting the link displays the detailed user contact information for the associated user. Handles must be unique, contact Uniform Resource Identifiers (URI) within the SES system domain. Users may have multiple handles to accommodate more that two personal points of contact to the user.

Note:

The SES system automatically appends the `@sip_domain.com` portion of the handle. Do not type this portion of the handle when adding or updating this end user on other screens.

Do not use the handles listed below for a user. They are reserved for system and administrator use:

- event-server
- cm-resubscribe
- confsvr
- presenceserver

In addition:

- Handles longer than 256 characters are truncated.
- If any of the preceding transformations produce handles already present, then they are dropped.
- No user handle may start with an underscore.
- All handles must be entered in lower case.
- All handles must be unique
- All handles must be alphanumeric and may contain a period, '-' (dash) or '_' (underscore)
- All handles must be between 3 and 16 ASCII characters.

User ID

(Optional) An identifier of at least three alphanumeric characters in length, used to authenticate a user to the SES system. Each user has one unique user ID, and, the User ID is the same as the user's handle. A User ID may be a name or an ID number.

Password, Confirm Password

(Required) Enter a password of at least 12 alphanumeric characters. Both field entries must match exactly.

Host

(Required) From the drop-down list of names, select the home server for this user. The host name of the current server is selected by default.

This is the name of the Converged Communications Server host serving the domain for this user. A host is a home or edge server or a combined home/edge server.

First Name, Last Name

(Required) This is the name of as many as 64 UTF-8 characters associated with this User ID and Handle in the user database. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

The name will be assigned to the speed dial button for this contact. In Japanese, this name string uses Kanji characters. (Contrast this with Alias).

Address 1, Address 2

(Optional) This is the first line and second line of the default address for users. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

The name will be assigned to the speed dial button for this contact. In Japanese, this name string uses Kanji characters. (Contrast this with Alias).

Office

Enter a designation for the user's office/floor, and so on, in alphanumeric characters

City

Enter the name of the city or town of the user's address in alphanumeric characters.

State

Enter the name of the state or province of the user's address in alphanumeric characters.

Country

Enter the name of the country of the user's address in alphanumeric characters.

ZIP

Enter the number of the ZIP or postal code of the user in numeric characters.

Add Media Server Extension

When you're using SIP trunking on one or more media servers running Avaya Communication Manager, you may select this field if you want to associate a new extension number with this user in the database now. If so, the Add Media Server screen on page 174 will be displayed next, after this user's profile has been added. If not, in the future you may choose to associate extensions with the user.

Add User screen command

Add

After entering/updating entries, select **Add** to submit the user's profile to the database on this host.

Search User screen

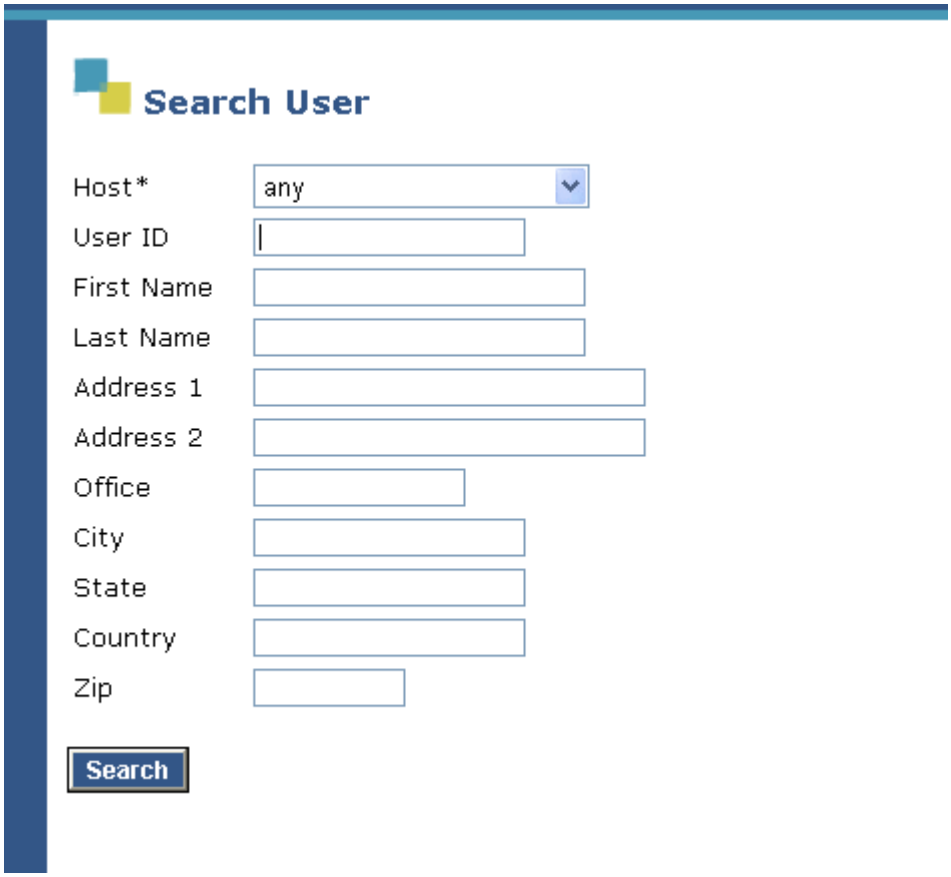
Locate any user on the system by searching on any of the fields in this screen.

On the left, open up the **Users** menu and select **Search** from the sub-menus to display the screen in Figure 54.

Choose a home server on which to search.

Fill in any of the fields to try and match. If any matches are found, the List Users screen that displays next shows only the matches.

Figure 54: Search Users screen



Search Users screen field descriptions

Host

(Required) This is the name of the home server for this user. You must know what home server the user has assigned.

By default, **any** is selected, which searches all the SES hosts you have administered for your enterprise.

The following fields allow for partial matches.

Enter a few characters to limit the results.

User ID

If you wish to search by ID, enter a valid User ID of at least 3 alphanumeric characters.
A User ID is an identifier of at least three alphanumeric characters in length, used to authenticate a user to the system. Each user has one unique user ID, and, the User ID is the same as the user's handle. A User ID may be a name or an ID number.

First Name, Last Name

If you wish to search by name, enter the given name or surname of the user in alphanumeric characters. (No punctuation is allowed.) This is the name of as many as 64 UTF-8 characters associated with this User ID and Handle in the user database. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

The name will be assigned to the speed dial button for this contact. In Japanese, this name string uses Kanji characters. (Contrast this with Alias).

Address 1, Address 2

If you wish to search by address, enter the first and/or second lines, respectively of the user's address in alphanumeric characters.

This is the first line and second line of the default address for users. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

The name will be assigned to the speed dial button for this contact. In Japanese, this name string uses Kanji characters. (Contrast this with Alias).

Office

Enter a designation for the user's office/floor, for example, in alphanumeric characters

City

Enter the name of the city or town of the user's address in alphanumeric characters.

State

Enter the name of the state or province of the user's address in alphanumeric characters.

Country

Enter the name of the country of the user's address in alphanumeric characters.

ZIP

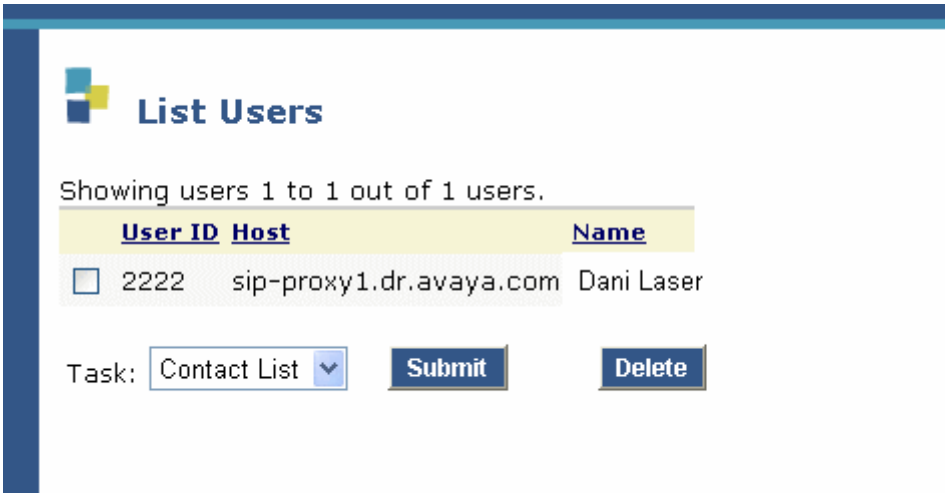
Enter the ZIP or postal code of the user in numeric characters.

Search Users screen field command

Search

After you've entered the information on which you want to match in the database, select **Search**.

Figure 55: Search Users result



Note that in this figure there is no Move User button. There is only one home server in the configuration, sip-proxy1, and so there is no other home to which the user may move.

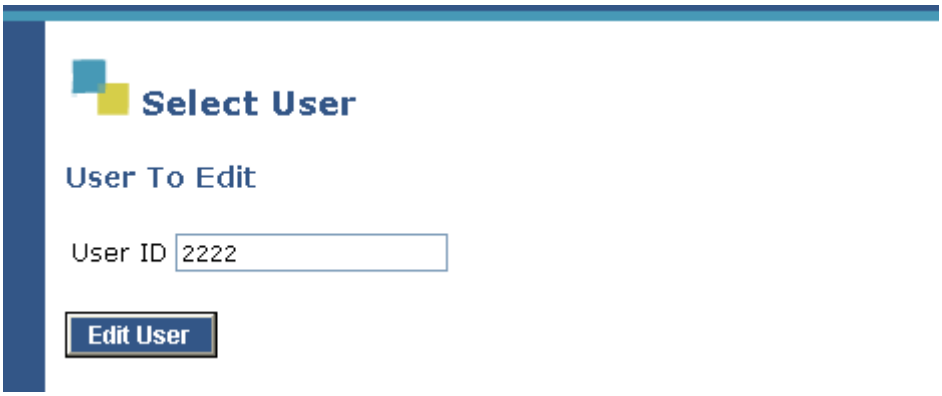
Select User screen

The Select User screen is available from the menu Users and three of its submenus:

- Users>Edit
- Users>Delete
- Users>Password

This click path provides a quick way to select a user for the tasks above when you are certain of the user's ID.

Figure 56: Select User screen



Note:

This interim screen allows you to specify a valid User ID in the database whose profile you wish to Edit or Delete, or for which you wish to update the Password.

Select User screen field description

User ID

(Required) An identifier of at least three alphanumeric characters in length, used to authenticate a user to the SES system. Each user has one unique user ID, and, the User ID is the same as the user's handle. A User ID may be a name or an ID number.

Select User screen commands

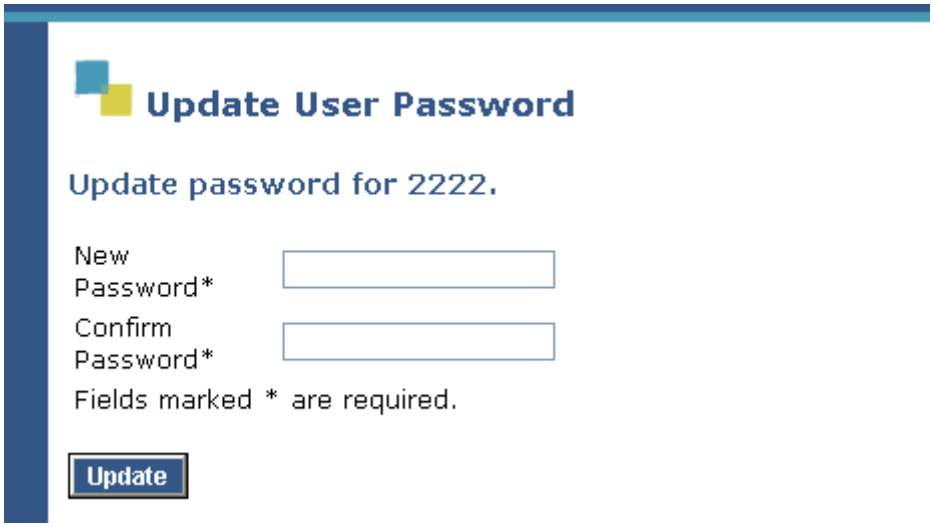
Edit User

Select Edit User to edit the user's profile.

Update Password screen

This is the screen on which you change a user's password for them. This screen is preceded by a the Select User screen that requires the user ID

Figure 57: Update User Password screen



Update Password screen field descriptions

User ID

(Read Only) An identifier of at least three alphanumeric characters in length, used to authenticate a user to the system.

New Password, Confirm Password

(Required) Enter a password of at least 6 and at most 12 alphanumeric characters. Both field entries must match exactly.

Update Password screen command

Update

After entering and confirming the new password, select **Update** to submit it to the host's database.

Edit User Profile screen

The User Profile screen contains specific demographic information about this user. This screen is originally populated by the default user profile data.

This screen now supports UTF-8 encoding. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

Figure 58: Edit User Profile screen

Edit User Profile screen field descriptions

User ID

(Required) An identifier of at least three alphanumeric characters in length, used to authenticate a user to the SES system. Each user has one unique user ID, and, the User ID is the same as the user's handle. A User ID may be a name or an ID number.

Password, Confirm Password

(Optional) Enter a password of at least 6 and at most 12 alphanumeric characters. Both field entries must match exactly.

Host

(Required) This is the name of the home server serving the domain for this user.

An administrator can move a user to a different home server. In the drop-down list, select a new host for this user. The user is deleted from the original database and moved to the other home server's database. See Moving a user to another home server on page 251.

First Name, Last Name

(Required) This is the name of as many as 64 UTF-8 characters associated with this User ID and Handle in the user database. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

The name will be assigned to the speed dial button for this contact. In Japanese, this name string uses Kanji characters. (Contrast this with Alias).

Address 1, Address 2

This is the first line and second line of the default address for users. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

The name will be assigned to the speed dial button for this contact. In Japanese, this name string uses Kanji characters. (Contrast this with Alias).

Office

Enter the designation for the user's office/floor, and so on, in alphanumeric characters.

Originally populated by the information in the Default User Profile screen, you can customize it here.

City

Enter the name of the city or town of the user's address in alphanumeric characters.

Originally populated by the information in the Default User Profile screen, you can customize it here.

State

Enter the name of the state or province of the user's address in alphanumeric characters.

Originally populated by the information in the Default User Profile screen, you can customize it here.

Country

Enter the name of the country of the user's address in alphanumeric characters.

Originally populated by the information in the Default User Profile screen, you can customize it here.

ZIP

Enter the number of the ZIP or postal code of the user in numeric characters.

Originally populated by the information in the Default User Profile screen, you can customize it here.

After entering/changing entries, select **Update** to submit the user's profile to the database on this host.

Edit User Profile screen command

Update

After entering the new information, select **Update** to submit it to the host's database.

Moving a user to another home server

In this procedure, the destination home server is fully functional.

If the user has a media server extension and the destination home server does *not* have an administered media server, the Move User operation cannot be completed. The move may only be completed if a media server is added to the destination home or the user's extension is removed or freed.

If your are moving a user to a home that links to a media server with more than one CLAN, you will be prompted to select one.

Move user can also be done from the List Users screen. See Moving a user to another home server on page 184.

1. From the Master Admin interface go to the Edit User Profile screen.
2. Select the Host field to display a drop-down menu of *all* home servers.

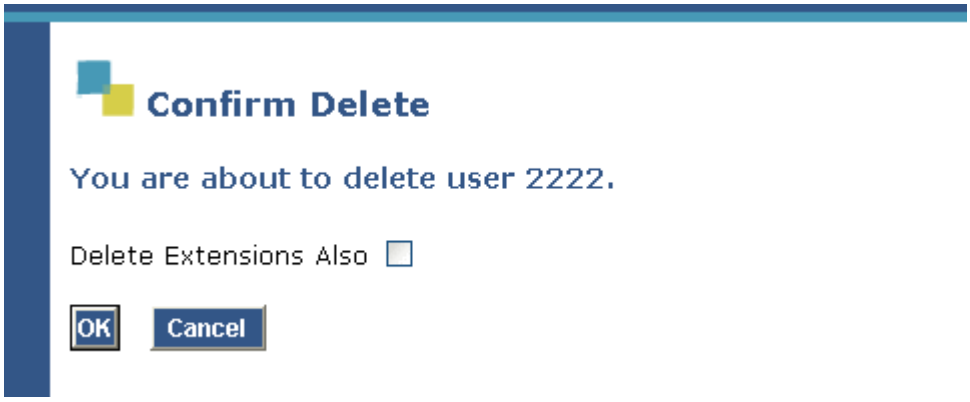
   The drop-down defaults to highlight the user's current home server.
3. Select another home server from the drop-down.

   If a home server connects to a media server that contains more than one media server interface, the drop-down menu displays both interfaces for you to choose from.
4. Select **Update**.
5. The system displays a Move User confirmation screen.
6. Press Accept or decline. OK or Cancel.
7. The system performs an update.
8. On Communication Manager, change the sip trunk for the extension of the user.
9. On the Toshiba Business Phone, SP-1020A, log out and log in.

Confirm Delete User screen

This screen is preceded by a Select User screen that requires the user ID of the user you want to delete.

Figure 59: Confirm Delete User screen



Confirm Delete User screen field descriptions

Confirm Delete

(Read Only) Informs you of which user you have selected for deletion from the database.

Confirm Delete User screen commands

Delete Extensions Also

Check this box to delete the media server extensions associated with this user. This user's extensions are deleted from the database as well. Leave the box unchecked, the default, to leave the unassociated extensions free for future use.

OK

Select **OK** to delete the user (and associated extensions, if applicable). See the example for the Confirm Delete User screen on page 252.

Cancel

Select **Cancel** to ignore your delete choices, keeping the user and associated extensions in the database unchanged.

Registered Users screen

This screen has two uses:

- Search for a specific user who is provisioned, registered, or both.
- Apply tasks to those users that meet the search criteria or to all users on this home server in the top part of the screen.

The Registered Users screen is available in both the Master Administrator interface and the Limited Administrator interface. This screen permits you to search, with the wild card asterisk (*) for users on a home server. You may search on any of the fields in the screen. Use the check boxes to include or exclude registered and provisioned users.

If a user has not received an extension number from the Communication Manager media server, that user will not be listed.

Figure 60: Registered Users search screen

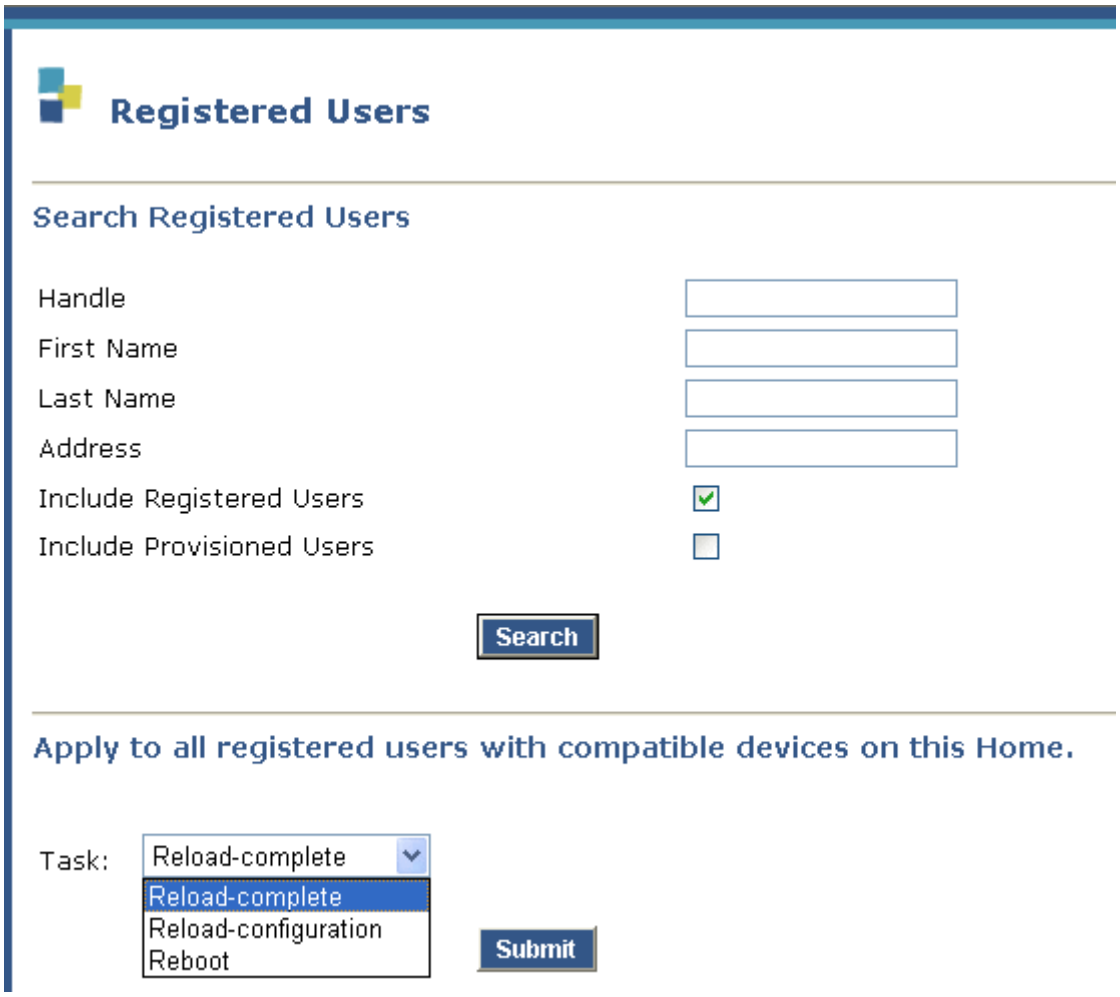


Figure 62 shows the result of the search criteria in Figure 60.

Figure 61: Registered User search result

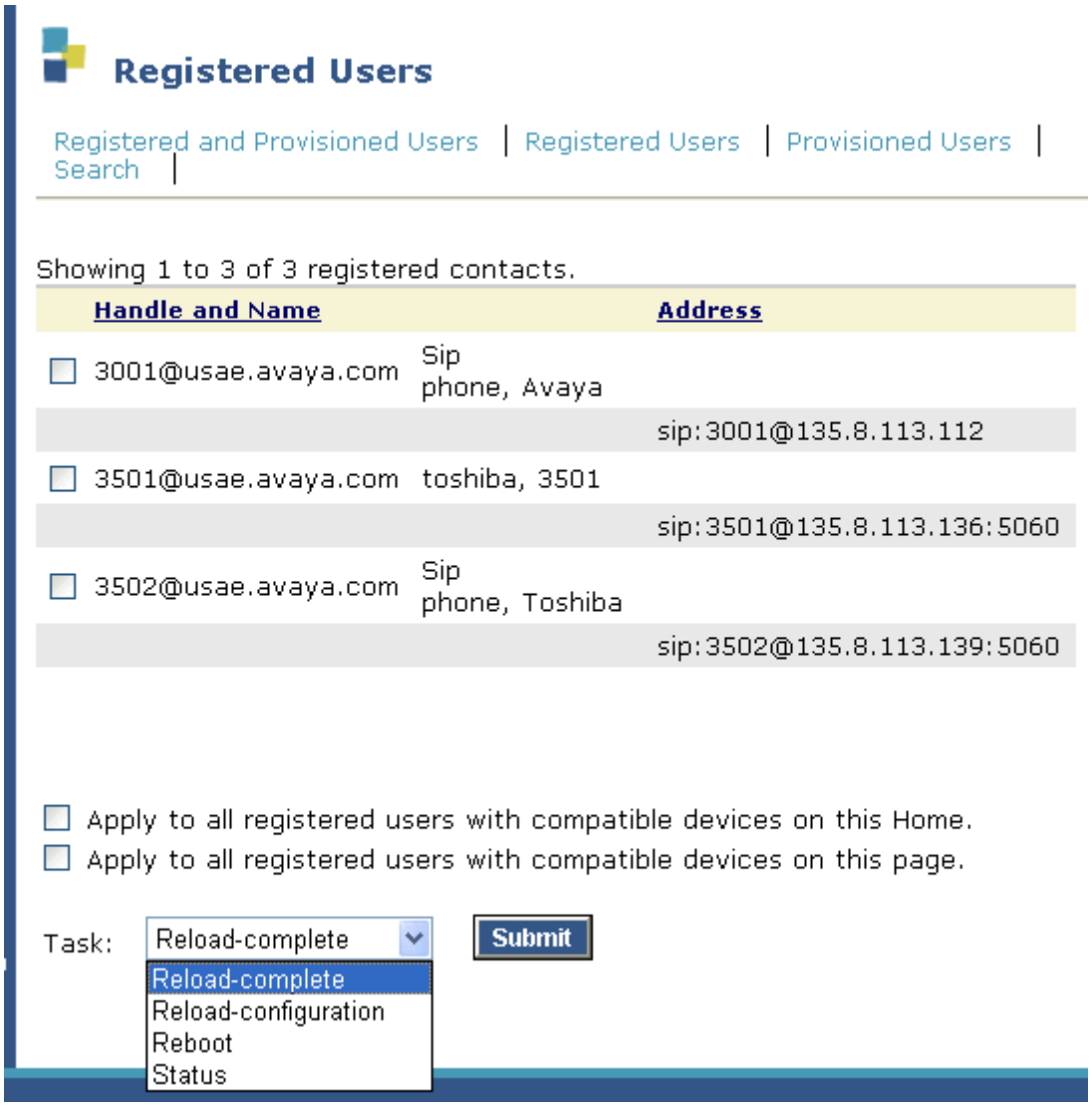
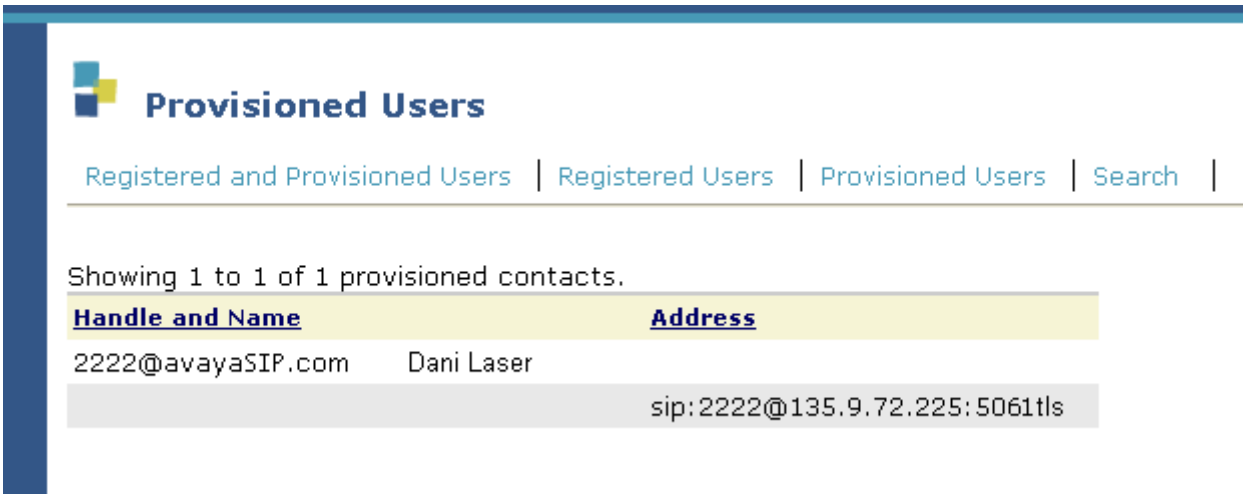
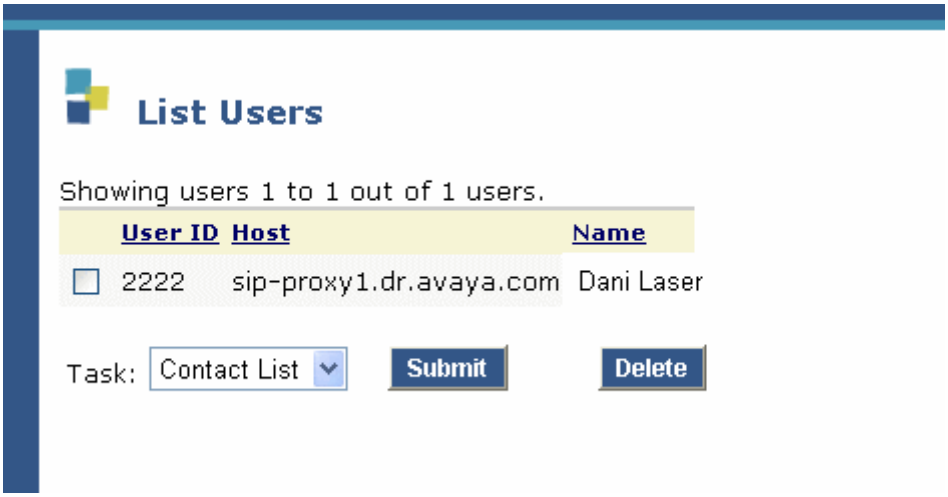


Figure 62: Registered User search result



If you perform a search from the user's list, or from Users > Search, the results show as in Figure 63.

Figure 63: Search Users result



Registered Users screen field descriptions

Handle

Enter a user's handle in this field, or at least two characters and a wild card asterisk to search for a user by a handle.

First Name, Last Name

Type at least two characters of a user's first or last name, then an optional wild card asterisk as search criteria.

This is the name of as many as 64 UTF-8 characters associated with this User ID and Handle in the user database. You may input Shift_JIS (SJIS) as well. Whether the browser sends UTF-8 or SJIS is dependent upon the browser's language setting.

The name will be assigned to the speed dial button for this contact. In Japanese, this name string uses Kanji characters. (Contrast this with Alias).

Address

In this screen, Address is the SIP contact address for registered users previously administered in the database. Type part of the address with an optional asterisk to search on this field.

Include Registered Users

Check this box to apply the search criteria above on registered users.

Include Provisioned Users

Check this box to apply the search criteria above on provisioned users.

Registered Users screen commands

Reload-complete task

Select this to completely reload software from the server to the device of all users selected.

Reload-configuration task

Select this to reconfigure the users' device for all selected.

Reboot task

Select this to instruct the users' device to reboot itself, that is, to reload its firmware for all selected.

Status task

Select this task to see a report of on hook and off hook status for the selected devices.

Submit

After choosing the task you want performed on the users that match the search criteria above, select Submit to begin the task.

In Figure 60: Registered Users search screen on page 254 and screens like it, the links at the top let you view groups of users:

- All registered and provisioned users
- All registered users
- All provisioned users

You may also search again.

Media Server Extensions

This section describes administering telephone extensions provided by the Communication Manager media server.

Administering Communication Manager extensions uses the edge server's Master Administrator interface. If you would like to manage a specific user's extension, see Extensions task on page 214. Access the Extensions screens through the Master Administration interface.

Manage Media Server Extensions screen

This menu has links to take you to the screens that list, add, and search for extensions on the media server.

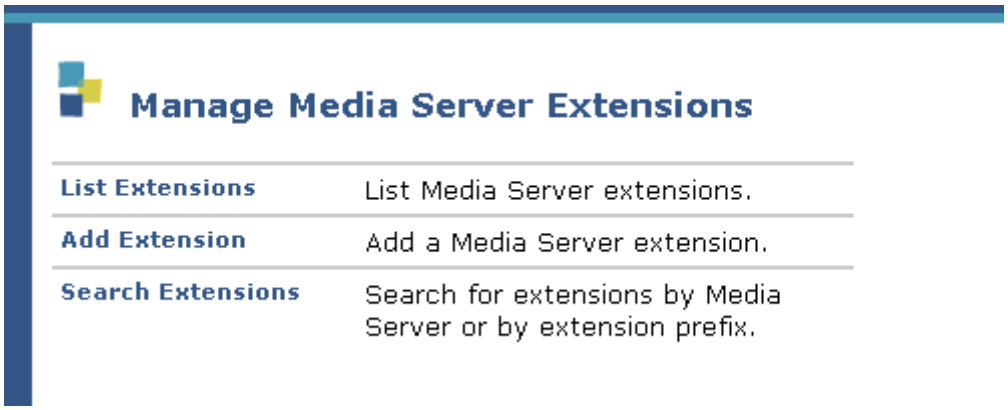
You may have to administer multiple CLANs if the media server associated with a home has more than one clan board.

Administering Multiple CLANs for a Communication Manager

Follow these steps:

1. If the Communication Manager associated with a home server has more than one clan board, then you must administer a media server interface for each clan present.
2. Select the **Media Server** link on the menu and add a media server interface for each clan board associated with the Communication Manager.
3. On the **Add Media Server** screen, the **Media Server Interface** field should contain a name to describe the clan, for example **clan1**.
4. Enter the IP address of the clan board in the **SIP Trunk IP Address** field.
5. Partition extensions across clans by assigning a unique set of extensions to each media server interface, logically distributing those extensions across users on that home server.

Figure 64: Manage Media Server Extensions screen



Manage Media Server Extensions screen field descriptions

List Extension

Select this link to go to the List Media Server Extensions screen on page 262 and view the administered telephone extensions.

Add Extension

Select this link to go to the Add Media Server Extension screen on page 266 and use an extension on the media server in the database. Extensions may be associated with users at the time they are created, or they may be created as free, and then associated with users in the future. Observe the following tips when creating extensions for users.

Tip:

Avaya highly recommends the following general user administration guidelines:

- Each SIP-enabled endpoint is administered as an off-premise station in Avaya Communication Manager. Verify that the trunk administered on the media server interface running Communication Manager for this OPS station correctly names this SES home host.
- Verify that the trunk associations with the OPS station matches Communication Manager trunk.

- Extensions for all users of Avaya SIP Softphone clients that are set up in Communication Manager must be added to SIP Enablement Services explicitly and associated with their User IDs. The Administration Without Hardware (AWOH) extension administered on the media server must match the extension administered in SIP Enablement Services. A match is required so that the users' SIP contact address, for example, `SIP:123456@mediaserver.domain.com`

  may be used as their handle as well.

- Extensions for all other users can be administered more easily using the patterns comprising address maps, the syntax of which is described in Pattern on page 302.

  For example, endpoints in your SES system currently use the prefix 543. The prefix of all users on the system must be changed to 987. Address maps advise the servers that any call directed to 538-0000 should be rerouted to 987-000.

Search Extensions

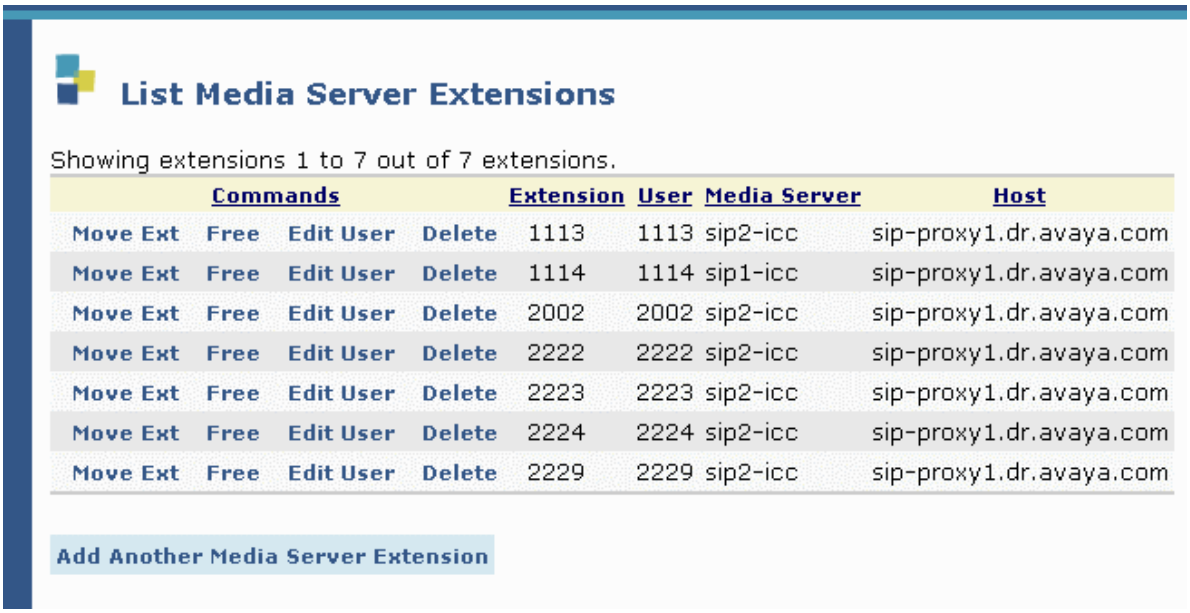
Select this link to go to the Search Media Server Extension screen on page 268 and find an extension by media server or prefix.

List Media Server Extensions screen

Use this screen to add a media server extension to an existing user in the database. You can create an extension or use a free one.

Manage the available extensions on the Communication Manager media server and assign or remove them from a user with this screen. This screen runs from the edge server's Master Administrator interface, but affects the Communication Manager media server.

Figure 65: List Media Server Extensions screen



List Media Server Extensions screen field descriptions

Extension

The numeric telephone extension in the database.

User

(Read Only) The name of the user associated with this telephone extension, if any. Blank if free.

Media Server

The name of the media server running Communication Manager.

Host

The home server managed by the media server named to the right.

List Media Server Extensions screen commands

Move Ext

Select this command to move a user's extension from being managed by one Communication Manager's CLAN interface to a different one.

Select the **Move Ext** command and the system displays the Select Media Server Interface for Extension screen as shown in Figure 66: Select Media Server Interface for Extension screen on page 264.

Free

This field only appears for extensions associated with users. Select this to disassociate this extension from the user, but leave the extension available so it can be reassigned to a user in the future.

Edit User

This field provides a convenient way to correct any errors in the user's profile. Selecting this displays the List Users screen on page 180, and let's you access all the user-related tasks in the pull-down menu there.

Delete

Select this to go to the **Confirm Delete Extension screen**. This will delete the extension from the media server.

Add Another Media Server Extension

Select this link to display the Add Media Server Extension screen on page 266 and assign extensions on the home to a media server.

Select Media Server Interface for Extension screen

Display this screen to move a user's extension for management by a different media server interface. For example, the prefix group of a user may be on one CLAN, but the user needs to be on a different media server because of the features it provides. This screen lets you administer that move.

Figure 66: Select Media Server Interface for Extension screen

Select Media Server Interface for Extension field descriptions

Extension

This is the extension you want to move to a different CLAN or PROCR media server interface.

Media Server Interface

This pull-down list contains the media server interfaces available to you. Select one.

Select Media Server Interface for Extension command

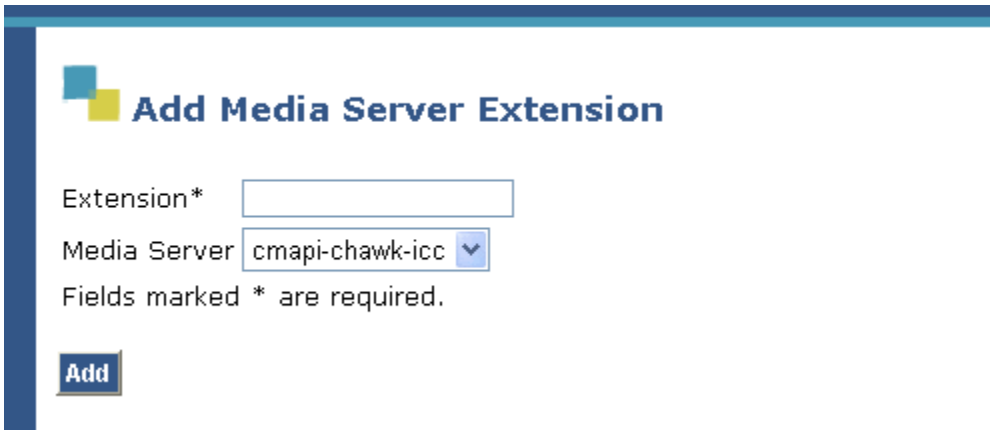
Submit

Click this button to make the change.

Add Media Server Extension screen

This screen lets you add an extension to a specific media server, helpful when it is necessary to combine two media servers, or change a user from one media server to another and not change the user's extension.

Figure 67: Add Media Server Extension screen



Add Media Server Extension screen field descriptions

Extension

(Required) The numeric telephone extension in the database.

Enter the numeric telephone extension you want to create in the database.

Media Server

(Read Only) Select the network name for the extension's media server interface from the drop-down list.

The node name in alphanumeric characters associated with the media server's CLAN (or processor CLAN) IP interface. Refer to "*Administration for Network Connectivity for Avaya Communication Manager,"* 555-233-504.

List Media Server Extension command

Add

Select **Add** to create a new entry for this media server extension in this SIP proxy server's database.

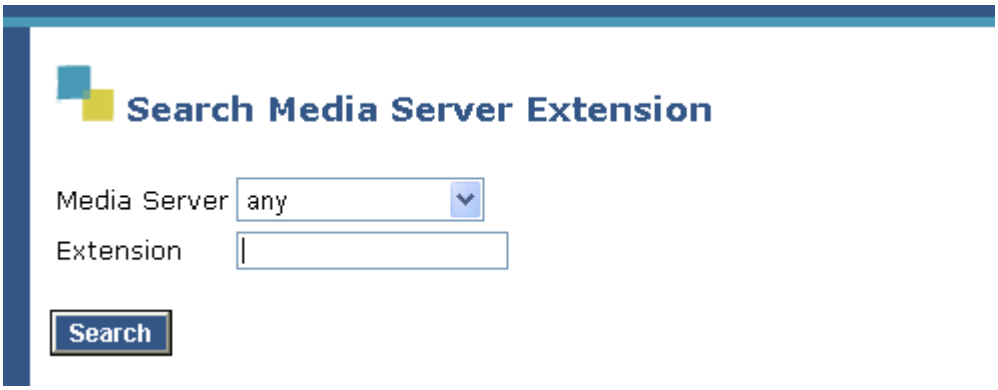
Note:

This will not create any extensions or change any existing administration performed directly through Avaya Communication Manager on the associated media server.

Search Media Server Extension screen

With this screen, search for extensions on a specific media server running Communication Manager.

Figure 68: Search Media Server Extensions screen



Search Media Server Extension screen field descriptions

Media Server

The node name in alphanumeric characters associated with the media server's CLAN (or processor CLAN) IP interface. Refer to "*Administration for Network Connectivity for Avaya Communication Manager,"* 555-233-504.

Select the name of the media server you want to search from the drop-down list of media servers. If you select the default **any**, the search checks all administered media servers.

Extension

(Required) The numeric telephone extension in the database.

Enter only a portion of the number, and the results of your search will be all extensions that match the entered digits.

Search Media Server Extension screen command

Search

After you've entered your pattern criteria, select **Search** to initiate your database query.

Emergency Contacts

On a media server, emergency endpoints can be managed with these screens.

These endpoints are designated as emergency contacts. Calls to these contacts do not require registration and are not authenticated.

These Emergency contacts are for the media server machine.

Edit Emergency Contact screen

You may change the emergency contact for the host at any time. Calls to this contact do not require registration and will not be authenticated.

Figure 69: Edit Emergency Contact screen

Edit Emergency Contact screen descriptions

Contact

(Required) The emergency **Contact** is an emergency username or extension. This field can be pre-populated or administered.

Host

(Read Only) The network name for the home/edge or home server associated with this contact.

Edit Emergency Contact screen command

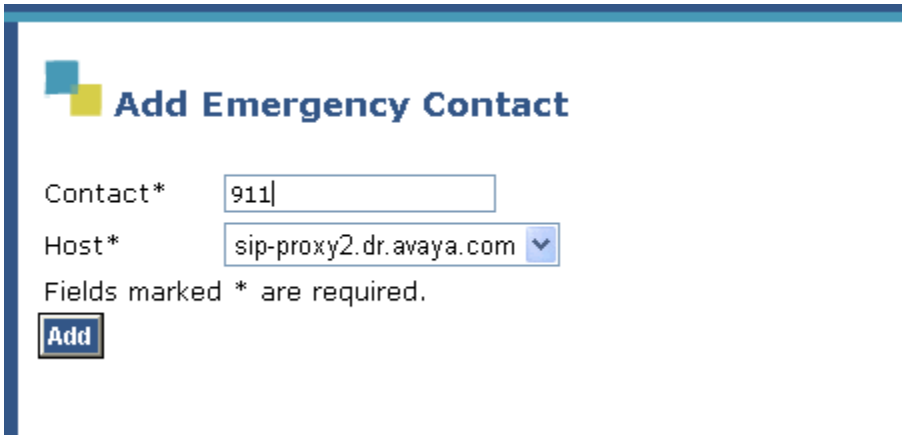
Update

Commit this change to the database

Add Emergency Contact screen

This screen lets you add emergency contacts to a SES host. If a user makes a call to this contact, the host waives registration and authentication.

Figure 70: Add Emergency Contact screen



Add Emergency Contact screen descriptions

Contact

(Required) The emergency **Contact** is an emergency username or extension. This field can be pre-populated or administered.

Host

(Required) Home server or home/edge server to which this emergency contact belongs.

Add Emergency Contact command

Add

Commit this change to the database.

List Emergency Contacts screen

The fields on this screen are discussed in Add Emergency Contact screen on page 271.

Calls to this URI do not require registration and will not be authenticated.

Figure 71: Emergency Contact List screen

List Emergency Contacts screen field descriptions

Contact

The emergency **Contact** is an emergency username or extension. This field can be pre-populated or administered.

Host

The **Host** field is the home/edge or home server with which the emergency URI is associated.

Host accepts a full SIP contact address or a partial URI, for example, just ***handle*** as in `handle@domain`.

List Emergency Contacts screen commands

Edit

Select the Edit command to display the Edit Emergency Contact screen on page 270. After edits are complete, the system displays the **List Emergency Contacts** screen.

Delete

After deleting, the system displays the **List Emergency Contacts** screen.

Add Another Emergency Contact

Select this to display the Add Emergency Contact screen on page 271.

Host screens

Host screens list, edit and add hosts to the SES system. This set of screens also allows administration of host address maps. A media server contact screen is placed within this set for your convenience.

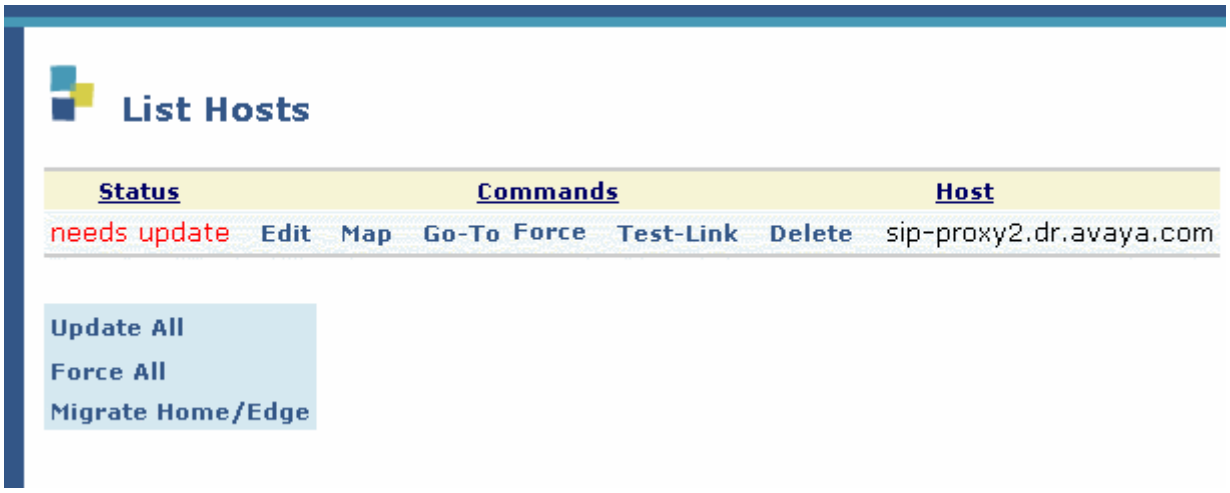
A host is any S8500 or S8500B hardware, that performs as an edge server, home/edge server, or home server.

Contrast with media server.

List Hosts screen

Check on the status with respect to synchronization of data between home and edge host servers with this screen.

Figure 72: List Hosts screen



List Hosts screen field descriptions

Status

(Read Only) Displays a message indicating if uncommitted updates exist since this server was last synchronized.

Host

(Read Only) The name for the edge, home, or home/edge host.

List Hosts screen commands

You may select any of the following links in the **Commands** field next to the name of a host.

Edit

Select **Edit** to use the Edit Hosts screen on page 277 for that host.

Map

Select **Map** to go to the Add Media Server Address Map screen on page 301, for that server.

Go To

Select **Go-To** to open a separate window that displays the target server's administrative web interface. This creates a session on that host to perform administrative tasks.

Force

Select **Force** to mandate an update on that server. Force updates the listed node only.

Test Link

Selecting **Test-Link** opens a window with a message indicating the status of connectivity to that server.

Delete

Select **Delete** to delete the host. This will fail if, for example, media server(s) use this host exclusively.

Update All

Select **Update All** to send database updates to other hosts in your system. If those databases are out of sync with the database on this host, select the Force All menu item to synchronize all hosts.

Update All propagates any changes you make from the Master Administrator interface. Update All is the routine mechanism to push data to the home servers. You do not need to limit its use.

Not executing Update All results in user data, edge data, and media server data not being pushed to the home servers. This non-synchronization ultimately causes many problems, users cannot log in, make calls, and so on.

For details on the use of Update All and Force All, see the appendix Force All and Update All use and behavior on page 471.

Force All

When an SES host is out of service, perhaps for maintenance, select **Force All** to synchronize the databases on all hosts. This choice may cause a temporary outage of service.

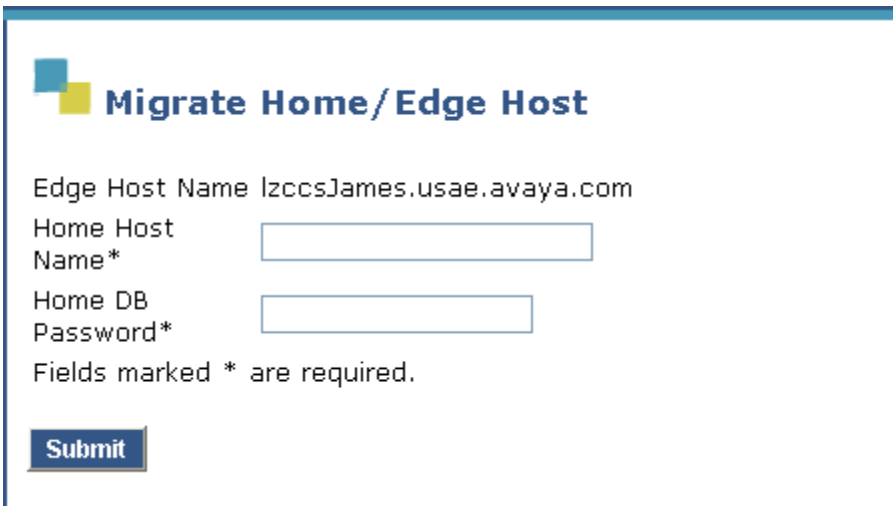
Force All completely wipes out the mvss database and reconstructs it. Select to use Force All only when you believe that user or system data are out of sync between the edge and home servers.

For details on the use of Update All and Force All, see the appendix Force All and Update All use and behavior on page 471.

Migrate Home/ Edge

Select this to change the current server from a combined home/edge configuration to distributed edge and home servers.

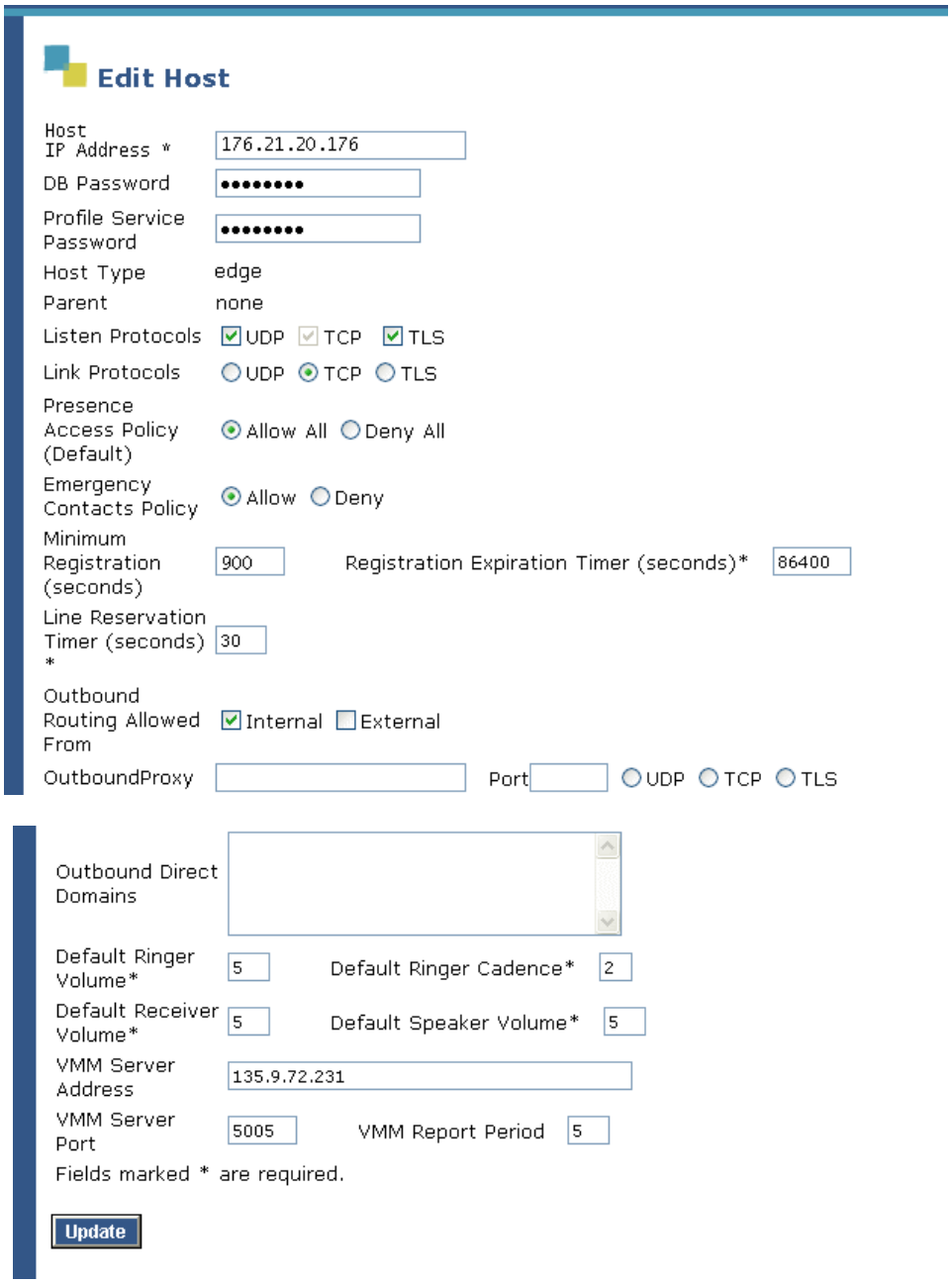
Figure 73: Migrate Home/Edge Host screen



Edit Hosts screen

Edit attributes of the host, including protocols, passwords, and system-wide rings and tones.

Figure 74: Edit Hosts screen



Edit Host screen field descriptions

See Add Host field descriptions Add Host screen on page 165.

Host IP Address

(Required) Enter the IP address for this edge, home, or home/edge server.

DB Password

(Required) Enter the password assigned to the database at installation, which should be at least 4 alphanumeric characters in length.

Profile Service Password

This password provides permissions between the SES hosts, both home server and edge server.

The Profile Service Password is not used by users or administrators. Rather, it is a password that uniquely identifies a proxy for intra- and inter-proxy communication. The Profile Service Password must be unique for each administered host.

Host Type

(Read Only) One of the following options is displayed:

- edge—if this is an edge proxy server for the SIP traffic of all domains
- home (this can appear only after an edge proxy is added)—if this is a home proxy to manage the SIP traffic of a specific domain
- home/edge—if this server functions as both your enterprise's edge and home proxies. Note that no additional proxy servers may exist within this architecture.

Parent

(Read Only) One of the following options is displayed:

- none—if an edge or home/edge is the server's Host Type, above.
- {HOST NAME}—if the server's Host Type field, above, is home, then the name of the edge proxy for all your enterprise's domains is listed as Parent.

Listen Protocols

At a minimum, select TLS for the **Listen Protocol**. You may select UDP or TCP for other uses, but Avaya Communication Manager only supports the TLS link protocol for SIP trunking.

Note that the protocol you select for linking must also be selected here for listening. At a minimum, you must select the protocol you selected as the **Link Protocol**, below, although you may want to select additional protocols only for listening but not for linking.

Link Protocols

This field refers to the trunk signaling between the Converged Communications Server R3.0 and Communication Manager. Typically, the selection here matches the Signal Group value on Communication Manager.

The only link protocol that is supported for SIP trunking with Avaya Communication Manager is TLS. For third-party proxy servers, you may select to link to SES with TLS, TCP, or UDP, although UDP is untested at this time.

You must also select the Link Protocol as a Listen Protocol, above. You may want to select additional listen protocols.

All three protocols are selected by default and available. There is no special reason to change the default.

Presence Access Policy

This setting correlates to the Watcher feature on the end user's SIP PIM web interface.

Accept the default policy of **Deny All**, or select **Allow All** to change this default policy and show the presence of SIP users on this server. The system displays the presence of SIP users on the SIP PPM web interface and on the Watchers screen.

The administrator may set a system policy to specify that all users on the system default to a blocked state, where users must authorize each other to view each other's presence. This may be overridden by the user's policy.

This administration policy is on a per node basis and may be administered for each home node in the network.

Emergency Contacts Policy

Enable this field to allow unauthenticated calls for the emergency contact named for this host.

If you allow emergency contacts, emergency calls can come to this host.

If you disable this field, unauthenticated calls to emergency URIs will be dropped.

Set up emergency URIs for the end user with the Add Emergency Contact screen.

Minimum Registration

The minimum registration timer is a SIP protocol feature that prevents endpoints from registering too quickly. Such a registration may be in error.

Enter a whole number of seconds, 900 through 59,940, that the SIP server should consider as the minimum acceptable duration value when a SIP client registers. If no value is entered, the default of 900 seconds is used.

Registration Expiration Timer

(Required) The value for Registration Expiration Timer determines how long a SIP endpoint should register for and renew its registration.

This value is not enforced by the registrar, but downloaded by an endpoint through PPM if they support it. The minimum registration time is enforced by the SIP registrar and it will not allow new registrations prior to that minimum registration time.The minimum registration timer is a SIP protocol feature that prevents endpoints from registering too quickly. Such a registration may be in error.

The default is 3, 600 seconds or 60 minutes.

This field affects all the users on this host.

Line Reservation Timer

(Required) This value is used to configure the maximum amount of time that an end user is allotted to dial a number after going off-hook. The default for this field is 30 seconds. The range is 30 to 240 seconds.

Outbound Routing Allowed From

Select Internal and/or External to specify whether SIP traffic can be routed only from endpoints internal to this server’s domain, or also from those external to it.

Outbound Proxy

Enter the hostname of the server within your enterprise that should manage SIP traffic bound for domains external to this server's domain. For example, on a home server, this would be the hostname of the edge that serves that home. On an edge/home or edge proxy server, an entry in this field typically is not required.

This field can contain the IP address of an edge for alternate use by a home.

Outbound Port

Enter the number of the port (1-65535) on the outbound proxy server specified above that should manage SIP traffic bound for domains external to this server's domain. **Port 5060** is recommended if the entry for Outbound Transport is TCP and **port 5061** if it is TLS.

Outbound Direct Domains

List those domains for which traffic may completely bypass the Outbound Proxy server specified above. For each domain, separate entries in the list with either commas or with a white space followed by a new line.

Default Ringer Volume

(Required) The value here determines how loudly the phone will ring for the entire system. Users can adjust their devices and override this.

The default is 5. The range is 1 to 10.

This field affects all the users on this host.

Default Ringer Cadence

(Required) The value in this field sets the cadence of the ring tone. The default is 2, the range for this field is 1 to 3.

This field affects all the users on this host, but can be adjusted by the user of a telephone.

Default Receiver Volume

(Required) This field sets the volume in the handset, rather than the speaker.

The default is 5. The range is 1 to 10.

This field affects all the users on this host.

Default Speaker Volume

(Required) This field sets the volume on the speaker rather than the handset.

The default is 5. The range is 1 to 10.

This field affects all the users on this host.

Voice Over IP Monitoring Manager (VMM) is a voice over IP (VoIP) quality of service (QoS) monitoring tool. This feature is available only on TSP SIP phones, model SP-1020A.

VMM information is taken from the VMM server. SES requires the server name, port address, and how frequenly an end point should report back to the VMM Server. See the VMM document Voice Over IP Monitoring Manager User Guide 555-233-510.

VMM Server Address

Address of the VMM server.

VMM Server Port

Port number for the VMM server's address.The range is 1 through 65,535, and the default is 5005.

VMM Report Period

The report period is in seconds, and reflects how often an end point should report back to the VMM server. Reports show jitter, round trip time, and packet loss. This may help in solving troubles on the SES network. The range is 5 through 30 seconds, and the default is 5 seconds.

Edit Hosts screen commands

Update

Select **Update** to submit your new or changed information to the server's database.

Host Address Map screens

The Host Address Map screens consist of these:

- List Host Address Map screen on page 283
- Add Host Address Map screen on page 286
- Edit Host Address Map screen on page 289

List Host Address Map screen

Address maps on the host let the server relate to endpoints that may be unfamiliar to them.

Go to this screen to see and change the address maps that are used by a specific host.

Figure 75: List Host Address Map screen

List Host Address Map screen field descriptions

Host

The network name for a home server.

Name

This is the name of the address map the home server should use.

Contact

Contact entries may be fixed (constant data you enter after you have selected **Edit**) or dynamically constructed by the system. In the example shown, the SES host has constructed a Contact dynamically by substituting *sip* as the protocol, *$*(user) to represent the user component in the original request URI, the IP address of the host (in this case, the home proxy server), and the port number and name of the transport to be used.

List Host Address Map screen commands

Edit (Address map)

Edit the host's address map as named with the Edit Host Address Map screen on page 289.

Delete (Address map)

Delete the address map on this host.

Edit (Contact)

Modify the contact information for the host hosting this address map. Edit Media Server Contact screen on page 312.

Add Another Map

See Add Host Address Map screen on page 286.

Delete (contact)

Deletes the contact named for this host.

Add Another Contact

Provide other contacts for this host with the Add Host Contact screen on page 292.

Delete Group

OK deletes a group on the host that has been set up for end user contacts.

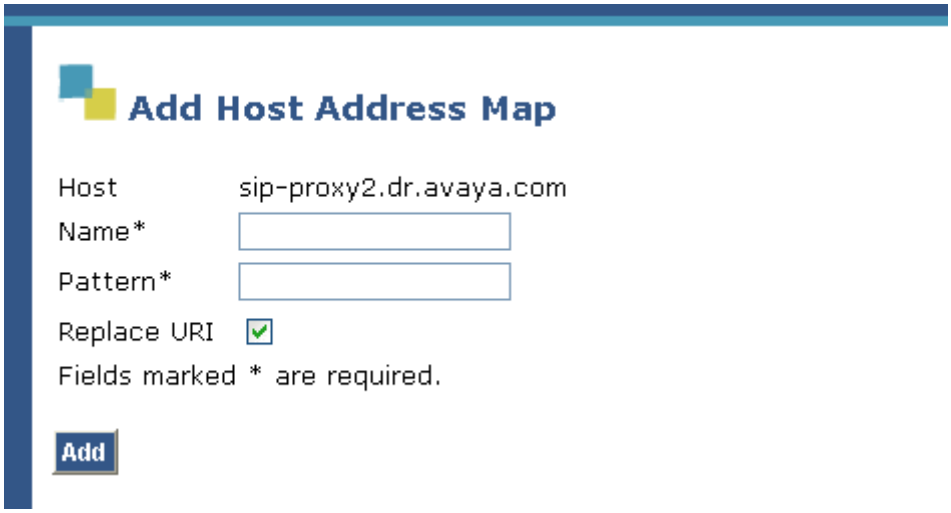
Add Map In New Group

Associate this address map in a new group. See Add Host Address Map screen on page 286.

Add Host Address Map screen

This is the screen to use if you want to add an address map for use by a home server. The address map correlates an endpoint to this home, particularly important with third-party endpoints on the combined system.

Figure 76: Add Host Address Map screen



Add Host Address Map screen field descriptions

Host

The network name for the home server.

Name

(Required) Enter the name of the address map you want this home server to use.

Pattern

(Required) This is a Linux regular expression that will match the extension numbers you wish to map. Regular expressions are a way to describe text through pattern matching. The regular expression is a string containing a combination of normal text characters, which match themselves, and special metacharacters, which may represent items like quantity, location or types of character(s). (NOTE: You do not need to match punctuation like dashes, periods or parentheses which may sometimes be used to enhance the readability of telephone extensions.) For example, [0-9] represents any single digit and * represents any number of digits or characters. So the example in the preceding illustration
^sip:538[0-9]*@customer.com
would match any SIP invite message (^ matches the beginning of a line) for any extension 3 or more digits in length, beginning with the digits 538, and ending with any other sequence of digits, in the customer.com domain.

An example of a pattern useful for matching outside-call messages would be
^sip:9[0-9]*@customer.com
which would match a SIP invite message for any length of dial string beginning with the digit 9.

Square brackets contain a selection of characters to be matched, with a hyphen indicating a range; so in our example,[0-9] matches any digit, or for another example, [13579] matches odd-numbered digits. Curly brackets which contain a whole number match that number of instances of the preceding item. So for example, 538[0-9]{4} matches any seven digits beginning with 538. Note that the braces may require escape characters: \{4\}

Another helpful metacharacter is dot (period), which matches any single character; for example, the regular expression.* matches any quantity of any character(s).

For more information, refer to "*SIP Support in Avaya Communication Manager*", Doc ID 555-245-206.

Add Host Address Map screen commands

Replace URI

The **Replace URI** is enabled by default because that is the correct selection in almost every circumstance. Select **Replace URI** to indicate that the contact named above should be resolved and forwarded by this proxy. This is the default, for this edge proxy to resolve and forward.

Deselect **Replace URI** if requests are to be forwarded to a *different* SIP proxy for resolution and routing.

Put another way, if the contact information must jump from edge proxy to edge proxy, Replace URI must *not* be checked. If the information only traverses within the local SIP-CM domains, Replace URI must be checked.

In case the contact information in this map is that of an endpoint, for example, a SIP phone or a user on a media server running Communication Manager, then this box should be checked. The box is checked by default, because the SIP proxy on a Converged Communications Server will overwrite the URI of the SIP request for these cases. If, however, you wish to configure this SES proxy to forward requests to another entity, that is, another SIP proxy server, for that entity to resolve the contact and route the request, then uncheck the **Replace URI** box.

Add

Submit your changes to the database.

Edit Host Address Map screen

Change the name of the host map, or the pattern used for generating SIP contact address with this screen.

See the discussion for Add Host Address Map screen on page 286.

Figure 77: Edit Host Map Entry

Edit Host Address Map screen field descriptions

Host

(Read only) The network name for the home server. This is the name in the drop-down list on the Host Address Map screen.

Name

(Required) Enter the name of the address map you want this home server to use.

Pattern

(Required) This is a Linux regular expression that will match the extension numbers you wish to map. Regular expressions are a way to describe text through pattern matching. The regular expression is a string containing a combination of normal text characters, which match themselves, and special metacharacters, which may represent items like quantity, location or types of character(s). (NOTE: You do not need to match punctuation like dashes, periods or parentheses which may sometimes be used to enhance the readability of telephone extensions.) For example, [0-9] represents any single digit and * represents any number of digits or characters. So the example in the preceding illustration

```
^sip:538[0-9]*@customer.com
```

would match any SIP invite message (^ matches the beginning of a line) for any extension 3 or more digits in length, beginning with the digits 538, and ending with any other sequence of digits, in the customer.com domain.

An example of a pattern useful for matching outside-call messages would be

```
^sip:9[0-9]*@customer.com
```

which would match a SIP invite message for any length of dial string beginning with the digit 9.

Square brackets contain a selection of characters to be matched, with a hyphen indicating a range; so in our example,[0-9] matches any digit, or for another example, [13579] matches odd-numbered digits. Curly brackets which contain a whole number match that number of instances of the preceding item. So for example, 538[0-9]{4} matches any seven digits beginning with 538. Note that the braces may require escape characters: \{4\}

Another helpful metacharacter is dot (period), which matches any single character; for example, the regular expression.* matches any quantity of any character(s).

For more information, refer to "*SIP Support in Avaya Communication Manager*", Doc ID 555-245-206.

Edit Host Address Map screen commands

Replace URI

The **Replace URI** is enabled by default because that is the correct selection in almost every circumstance. Select **Replace URI** to indicate that the contact named above should be resolved and forwarded by this proxy. This is the default, for this edge proxy to resolve and forward.

Deselect **Replace URI** if requests are to be forwarded to a *different* SIP proxy for resolution and routing.

Put another way, if the contact information must jump from edge proxy to edge proxy, Replace URI must *not* be checked. If the information only traverses within the local SIP-CM domains, Replace URI must be checked.

In case the contact information in this map is that of an endpoint, for example, a SIP phone or a user on a media server running Communication Manager, then this box should be checked. The box is checked by default, because the SIP proxy on a Converged Communications Server will overwrite the URI of the SIP request for these cases. If, however, you wish to configure this SES proxy to forward requests to another entity, that is, another SIP proxy server, for that entity to resolve the contact and route the request, then uncheck the **Replace URI** box.

Update

Submit your changes to the database.

Host Contact screens

Host Contact screens consist of these:

- Add Host Contact screen on page 292
- Edit Host Contact screen on page 294

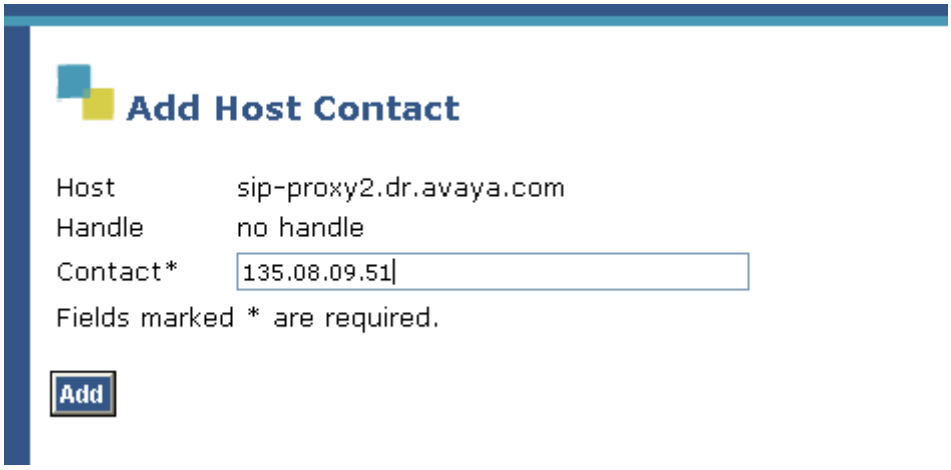
Add Host Contact screen

The information on this screen routes traffic to another home server based on a handle.

This screen provides a contact pattern for the host machine on which an address map exists to the to route SIP traffic to an alternate host, based on the pattern in the Contact field.

See the discussion for List Host Address Map screen on page 283, Add Another Contact field.

Figure 78: Add Host Contact screen



Add Host Contact screen field descriptions

Host

(Read only) The network name for the home server that has authority over this user.

Handle

On this screen, **Handle** means the friendly name of the home server shown just above.

Contact

(Required) In this field, enter the IP address or FQDN of a media server running Communication Manager.

Contact entries may be fixed (constant data you enter after you have selected **Edit**) or dynamically constructed by the system. In the example shown, the SES host has constructed a Contact dynamically by substituting *sip* as the protocol, *$*(user) to represent the user component in the original request URI, the IP address of the host (in this case, the home proxy server), and the port number and name of the transport to be used.

Add Host Contact screen commands

Add

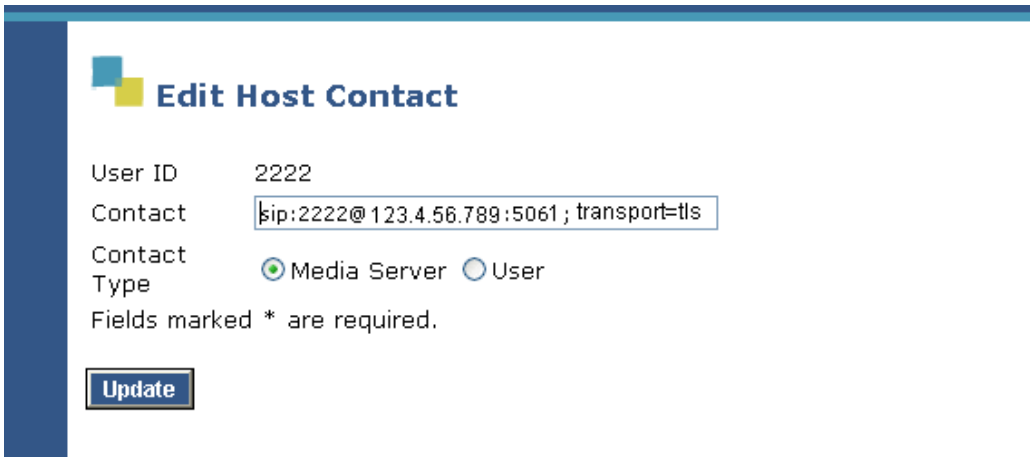
Commit the information to the database.

Edit Host Contact screen

This screen provides a home or home/edge contact for the edge server.

This information is required so that the media server is accessible when an address map exists for this host.

Figure 79: Edit Host Contact screen



Edit Host Contact screen field descriptions

Host

(Read only) On this screen, the Host field contains the name of the edge server that serves the home or home/edge server you enter below.

Contact

(Required) Enter the name of a home or home/edge server this media server should access.

Edit Host Contact screen commands

Update

Commit this change to the database.

Media Server screens

This series of screens lets you administer aspects of the media server running Communication Manager.

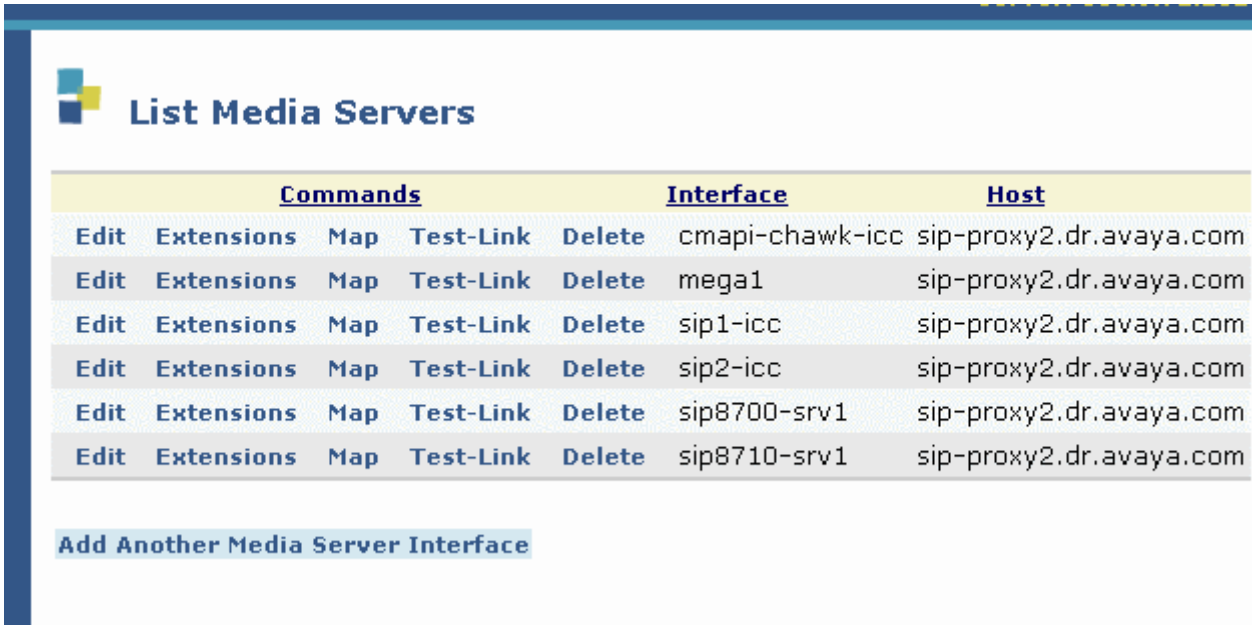
- List Media Servers screen on page 295
- Add Media Server screen on page 174
- Edit Media Server screen on page 298

Communication Manager media server address maps are not required if all of the endpoints in the system reside on the Communication Manager media server. Because all endpoints are known by the system, the SIP message is correctly routed to the correct endpoint.

List Media Servers screen

This screen shows all of the Communication Manager media servers in the system.

Figure 80: List Media Servers screen



List Media Servers screen field descriptions

Interface

(Read only) Name of the media server running Communication Manager's processor CLAN that serves the hosts listed.

Host

(Read only) The alphanumeric name for this home server.

To administer a new media server in the proxy host's database, select **Add Another Media Server**.

List Media Server screen commands

You may select any of the following links in the **Commands** field next to a media server's name.

Edit

Select **Edit** to display the Edit Media Server screen on page 298. The **Edit Media Server** screen allows changes to the server name, host, link type, passwords, IP addresses, and more.

Extensions

This command relates to the telephone extensions on the media server. Select **Extensions** to view the List Media Server Extensions screen on page 262, for this media server. With this screen, you can free, delete entirely, or change what user is assigned to a particular extension on the media server.

Map

Select **Map** to display the List Media Server Address Map screen on page 304, for that media server

Test Link

Select **Test Link** to open a window with a message indicating the status of connectivity from the media server to its host. Select **Close** when finished viewing the status.

Delete

Select **Delete** to go to the **Confirm Delete Media Server** screen. Verify that you want to delete the media server.

Add Another Media Server

Add another media server to serve another edge server. Select this command to display the Add Media Server screen on page 174.

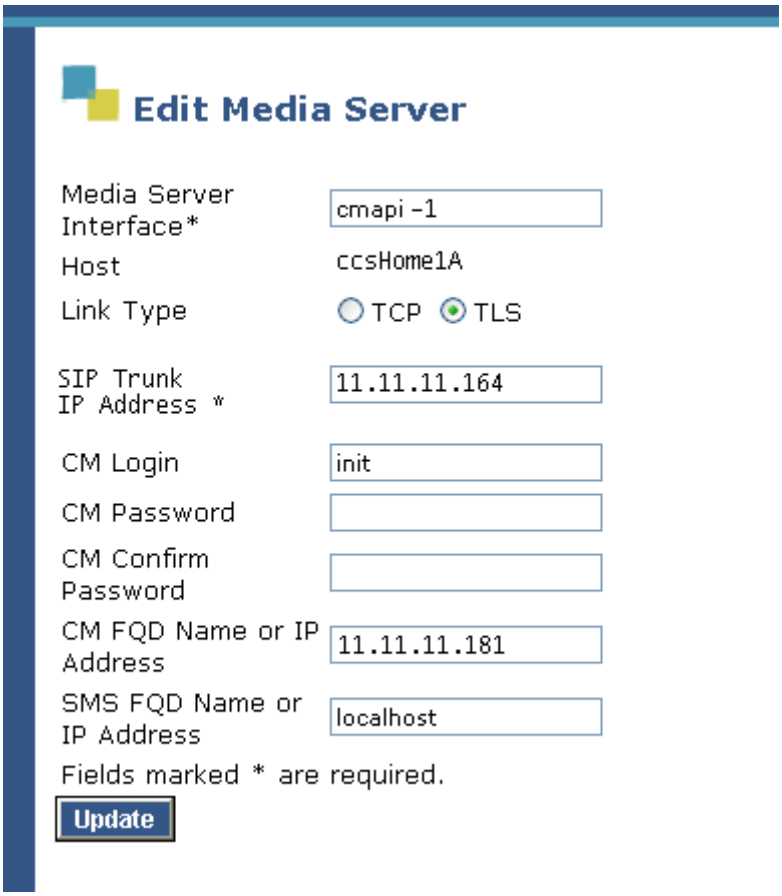
Add Media Servers screen

See Add Media Server screen on page 174 for a discussion of this screen.

Edit Media Server screen

This screen assigns home servers to a media server interface.

Figure 81: Edit Media Servers screen



Edit Media Server screen field descriptions

Media Server Interface

(Required) Enter a friendly name in alphanumeric characters for the media server's CLAN (or processor CLAN) IP interface. You may wish to use the same name as is used for this media server on the **IP Node Names** screen in Communication Manager. Each media server's name must be unique.

If the media server itself has more than one CLAN interface you must add home servers to each one.

Host

(Read Only) In this screen, the Host field displays the name of the home server for whose users the media server specified above is the default.

Link Type

Select one of the listed protocols as the one to be used to link the media server with the specified host:

- TCP (Transport Control Protocol)—if this protocol is not an option for your system, then the Link Type field may not appear on this screen.
- TLS (Transport Link Security)—this is the default protocol which is selected for all servers.

SIP Trunk IP Address

(Required) This field holds the IP address for the media server's CLAN. This field names the link that supports the SIP trunk. The IP address must be specified as a 32-bit address comprising four 8-bit octets (for example, 'xxx.xxx.xxx.xxx' where 'xxx' is a value of 0-255) . If DNS is available within its domain, the fully qualified domain name of the media server's CLAN (or processor CLAN) may be entered.

CM Login

Login for the Communication Manager software. Your login should be of type **customer** and service level **superuser** at a minimum. Understand that this has to be set for every media server running Communication Manager.

CM Password / CM Password Confirm

Password for the Communication Manager software.

CM FQD Name or IP Address

The IP address or the fully qualified domain name, or the native NIC or other administered interface in IP services form on the Communication Manager's CLAN or processor CLAN of the server that holds Communication Manager. This field is for the link that supports SAT commands with the media server's name.

SMS FQD Name or IP Address

The IP address or the fully qualified domain name (host name) of the systems management server.

Edit Media Server screen command

Update

Commit the information on this screen to the database.

Media Server Address Map screens

There are three screens for administering the media server address maps, Add, List, and Edit.

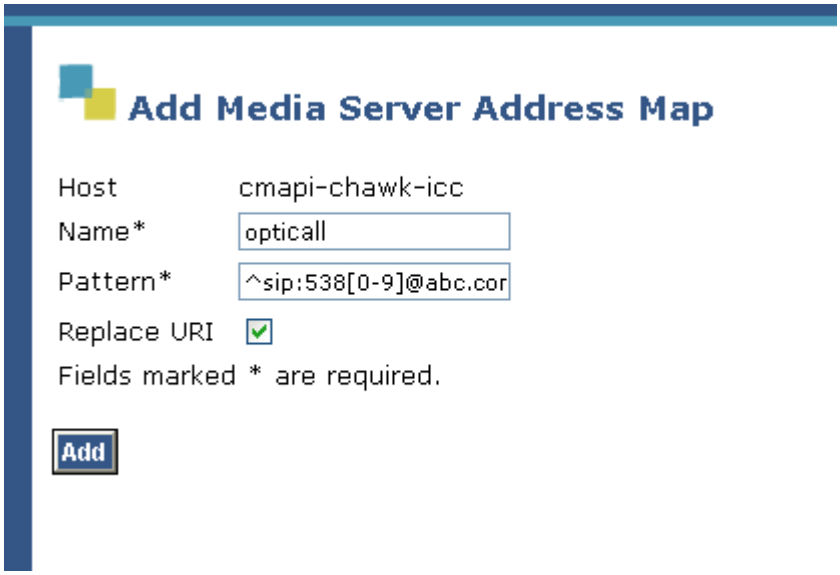
- Add Media Server Address Map screen on page 301
- List Media Server Address Map screen on page 304
- Edit Media Server Address Map screen on page 307

Add Media Server Address Map screen

Use this screen to create an address map for a media server and its home server.

If all endpoints in your SIP domain are Avaya soft phones with OPTIM/OPS administered on the Communication Manager, these media server maps are not needed.

Figure 82: Add Media Server Address Map screen



Add Media Server Address Map screen field descriptions

Note:

An address map identifies the messages allowed between SES host servers running SES and the media server running Communication Manager. These messages travel over the SIP trunk administered in Communication Manager. Devise map patterns to specify the allowed messages clearly. If a map does not clearly identify the allowed message string, especially when the map uses wild-card metacharacters, then unnecessary data may flow to Communication Manager.

For example, an address map pattern of **^sip:13*** may match many IP addresses in the network, resulting in much unintended messaging traffic over that SIP trunk. If presence isn't working properly in your IM client, check that the patterns in your address maps are clear and correct.

Host

(Read Only) On this screen, the Host field displays the name of the media server to which this address map applies. This field does not refer to either an edge or home host.

Name

(Required) The name of the address map.

Enter an alphanumeric name to identify the address map you are adding to this Communication Manager media server. This is not a network name, but might be a way of identifying to which set of extensions on which Communication Manager media server the map applies.

Pattern

(Required) This is a Linux regular expression that will match the extension numbers you wish to map. Regular expressions are a way to describe text through pattern matching. The regular expression is a string containing a combination of normal text characters, which match themselves, and special metacharacters, which may represent items like quantity, location or types of character(s). (NOTE: You do not need to match punctuation like dashes, periods or parentheses which may sometimes be used to enhance the readability of telephone extensions.) For example, [0-9] represents any single digit and * represents any number of digits or characters. So the example in the preceding illustration
^sip:538[0-9]*@customer.com
would match any SIP invite message (^ matches the beginning of a line) for any extension 3 or more digits in length, beginning with the digits 538, and ending with any other sequence of digits, in the customer.com domain.

An example of a pattern useful for matching outside-call messages would be
^sip:9[0-9]*@customer.com
which would match a SIP invite message for any length of dial string beginning with the digit 9.

Square brackets contain a selection of characters to be matched, with a hyphen indicating a range; so in our example,[0-9] matches any digit, or for another example, [13579] matches odd-numbered digits. Curly brackets which contain a whole number match that number of instances of the preceding item. So for example, 538[0-9]{4} matches any seven digits beginning with 538. Note that the braces may require escape characters: \{4\}

Another helpful metacharacter is dot (period), which matches any single character; for example, the regular expression.* matches any quantity of any character(s).

For more information, refer to "*SIP Support in Avaya Communication Manager*", Doc ID 555-245-206.

Replace URI

The **Replace URI** is enabled by default because that is the correct selection in almost every circumstance. Select **Replace URI** to indicate that the contact named above should be resolved and forwarded by this proxy. This is the default, for this edge proxy to resolve and forward.

Deselect **Replace URI** if requests are to be forwarded to a *different* SIP proxy for resolution and routing.

Put another way, if the contact information must jump from edge proxy to edge proxy, Replace URI must *not* be checked. If the information only traverses within the local SIP-CM domains, Replace URI must be checked.

In case the contact information in this map is that of an endpoint, for example, a SIP phone or a user on a media server running Communication Manager, then this box should be checked. The box is checked by default, because the SIP proxy on a Converged Communications Server will overwrite the URI of the SIP request for these cases. If, however, you wish to configure this SES proxy to forward requests to another entity, that is, another SIP proxy server, for that entity to resolve the contact and route the request, then uncheck the **Replace URI** box.

Add Media Server Address Map screen commands

Add

Commit the change to the database.

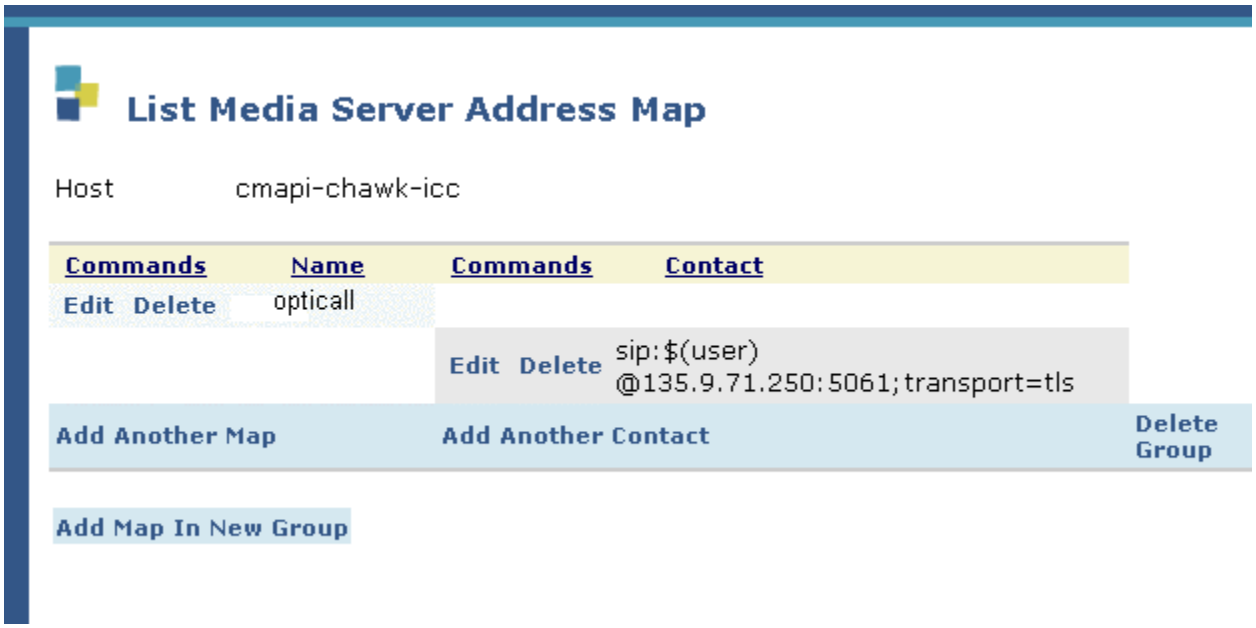
List Media Server Address Map screen

Address maps for media servers are listed in groups and are associated with media servers and the extensions on them.

This screen, Figure 83, shows the current address maps for the media server cmap-chawk-icc. With this screen you can manage maps, contacts, and groups on the media server.

If all endpoints in your SIP domain are Avaya soft phones with OPTIM/OPS administered on the Communication Manager, a media server maps is not needed.

Figure 83: List Media Server Address Map screen



List Address Map screen field descriptions

Host (Media Server name)

(Read Only) On this screen, next to the Host label is the name of the media server to which this address map applies. This field does not refer to either an edge or home host.

Name

(Read Only) The name of the address map.

Contact

Contact entries may be fixed (constant data you enter after selected **Edit**) or dynamically constructed by the system. In the example shown, the host has constructed a Contact dynamically by substituting sip as the protocol, $(user) to represent the user component in the original request URI, the IP address of the host (in this case, the home proxy server), and the port number and name of the transport to be used.

List Address Map screen commands

You may select any of the following links in the Commands field next to a map's Name or an associated Contact:

Edit (Addr Map)

Edit the map entry with the Edit Media Server Address Map screen on page 307. Edit the contact for the media server. Use the Edit Media Server Contact screen on page 312 for that contact in the database.

Delete (Addr Map)

To confirm your deletion, go to the **Confirm Delete Map** screen for that map or the **Confirm Delete Contact** screen for that Contact in the database.

Edit (Contact)

This displays and permits changing the address of the host this media server is associated with.

Delete (Contact)

This field lets you delete the association between the SES home server and the Communication Manager media server.

Add Another Map

Select the **Add Another Map** to add another address map to this media server.

Add Another Contact

Select **Add Another Contact** to apply another address map to route a home server to.

Delete Group

Select the **Delete Group** link to remove this group of address map(s) from the database.

Add Map in New Group

Or select the **Add Map in New Group** link to create a new address map in a new group.

Edit Media Server Address Map screen

You may need to edit the name of a media server's map entry or change the pattern for that map.

If all endpoints in your SIP domain are Avaya soft phones with OPTIM/OPS administered on the Communication Manager, media server maps are not needed.

Figure 84: Edit Media Server Map Entry screen

Note:

An address map identifies messages allowed between the SES host server and the media server over the SIP trunk administered in Avaya Communication Manager. Choose your map patterns to specify the allowed messages clearly. If a map does not clearly identify the allowed message string (especially when the map uses wild-card metacharacters), then unnecessary data may flow to Communication Manager. For example, an address map pattern of `^sip:13*` may match many IP addresses in the network, resulting in much unintended messaging traffic over that SIP trunk. If presence isn't working properly in your IM client, check that the patterns in your address maps are clear and correct.

Edit Media Server Address Map screen field descriptions

Host

(Read Only) On this screen, next to the Host label is the name of the media server to which this address map applies. This field does not refer to either an edge or home host.

Name

(Required) The name of the address map.

Enter an alphanumeric name to identify the address map you want to edit. This is not a network name, but might be a way of identifying to which set of extensions on which media server the map applies.

Pattern

(Required) This is a Linux regular expression that will match the extension numbers you wish to map. Regular expressions are a way to describe text through pattern matching. The regular expression is a string containing a combination of normal text characters, which match themselves, and special metacharacters, which may represent items like quantity, location or types of character(s). (NOTE: You do not need to match punctuation like dashes, periods or parentheses which may sometimes be used to enhance the readability of telephone extensions.) For example, [0-9] represents any single digit and * represents any number of digits or characters. So the example in the preceding illustration
^sip:538[0-9]*@customer.com
would match any SIP invite message (^ matches the beginning of a line) for any extension 3 or more digits in length, beginning with the digits 538, and ending with any other sequence of digits, in the customer.com domain.

An example of a pattern useful for matching outside-call messages would be
^sip:9[0-9]*@customer.com
which would match a SIP invite message for any length of dial string beginning with the digit 9.

Square brackets contain a selection of characters to be matched, with a hyphen indicating a range; so in our example,[0-9] matches any digit, or for another example, [13579] matches odd-numbered digits. Curly brackets which contain a whole number match that number of instances of the preceding item. So for example, 538[0-9]{4} matches any seven digits beginning with 538. Note that the braces may require escape characters: \{4\}

Another helpful metacharacter is dot (period), which matches any single character; for example, the regular expression.* matches any quantity of any character(s).

For more information, refer to "*SIP Support in Avaya Communication Manager*", Doc ID 555-245-206.

Replace URI

The **Replace URI** is enabled by default because that is the correct selection in almost every circumstance. Select **Replace URI** to indicate that the contact named above should be resolved and forwarded by this proxy. This is the default, for this edge proxy to resolve and forward.

Deselect **Replace URI** if requests are to be forwarded to a *different* SIP proxy for resolution and routing.

Put another way, if the contact information must jump from edge proxy to edge proxy, Replace URI must *not* be checked. If the information only traverses within the local SIP-CM domains, Replace URI must be checked.

In case the contact information in this map is that of an endpoint, for example, a SIP phone or a user on a media server running Communication Manager, then this box should be checked. The box is checked by default, because the SIP proxy on a Converged Communications Server will overwrite the URI of the SIP request for these cases. If, however, you wish to configure this SES proxy to forward requests to another entity, that is, another SIP proxy server, for that entity to resolve the contact and route the request, then uncheck the **Replace URI** box.

Edit Media Server Address Map screen commands

Update

After reviewing and/or changing the entries in one or more of the fields, select **Update** to submit the address map entry to the database on this host.

Media Server Contact screens

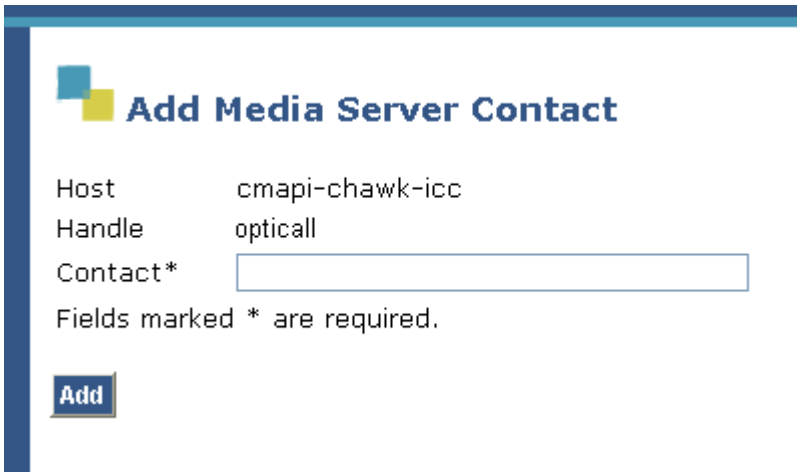
The Media Server Contact screens let you create and change the way you route traffic to a different media server interface than the one specified on the Media Server screen.

- Add Media Server Contact screen on page 310
- Edit Media Server Contact screen on page 312

Add Media Server Contact screen

Use this screen to route traffic to another media server interface than the one specified on the Media Server screen. You will apply an address map to accomplish this.

Figure 85: Add Media Server Contact screen



Add Media Server Contact screen descriptions

Host (Media server name)

(Read Only) In this screen, this is the name of the Communication Manager media server interface to which you are associating a SES host server.

Handle (name of address map)

(Read Only) In this screen, this is the name of the address map you are adding.

Contact

(Required) In this field, identify the edge host associated with the media server named above. Use either an IP address or fully qualified domain name (host name). This is not the usual definition of Contact as used so far.

Add Media Server Contact screen commands

Add

Select this link to commit the new data to the database.

Edit Media Server Contact screen

If you need to change the address map information for the Communication Manager media server, use this screen

Figure 86: Edit Media Server Contact screen

Edit Media Server Contact screen field descriptions

Host (media server)

(Read Only) Displays the name of the Communication Manager media server to which this contact applies.

Contact

Enter the fully qualified domain name, host name, or IP address of an edge server.

When a match for an address map is found, the associated Contact may be a fixed destination, and is constructed dynamically from the Add Media Server Map and associated entries. This contact must include any of the components in the original SIP request URI. The latter is accomplished using the syntax $(component-name). The syntax of a SIP contact address (including its optional components) is as follows:

```
protocol:user:password@host:port;uri-parameters?headers
```

In the example shown, the proxy host has constructed a Contact by substituting **sip** as the protocol, $(user) to represent the user in the original request URI, the IP address of the host (in this case, the home proxy server), the port number for the transport to be used, and the name of the transport.

Edit Media Server Contact screen command

Update

After reviewing and perhaps changing it, select the Update button to submit the entry to the host database.

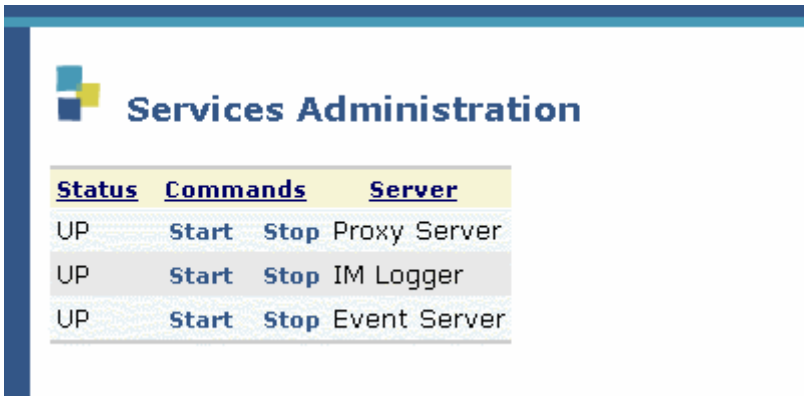
Services screen

At this time there is one services screen available to check the up or down status of a server, and to turn a server on or off.

Services Administration screen

This screen shows the status of the event server, the home server, and edge servers in the SIP domain. No information about the media server is available on this screen.

Figure 87: Services Administration screen



Services Administration screen field descriptions

Status

(Read Only) Displays a message indicating whether each required service is running on this server. The possible messages are:

- **?**—if the status of this service is unknown to the Administration web interface at this time
- **UP** (or Started)—if this service is running on this host. This message indicates the normal state for a properly functioning server
- **DOWN** (or Stopped)—if this service is not running on this host. This message may indicate a problem with the server, its installation or configuration.
- **Partially Up**—some process have started, but not all. A transitional status. Wait.
- **Off**—the server has been turned off or is not yet started.

Server

(Read Only) Shows the names for each of the required services on this host:

- Proxy Server—this represents the proxy-related services for this SIP server
- IM Logger—this represents the services related to the instant-messaging log facility
- eventserver—this represents the service handling events

Services Administration screen commands

Start

Starts this service on this host, if it is not running.

Stop

Stops the service on the host if it is running.

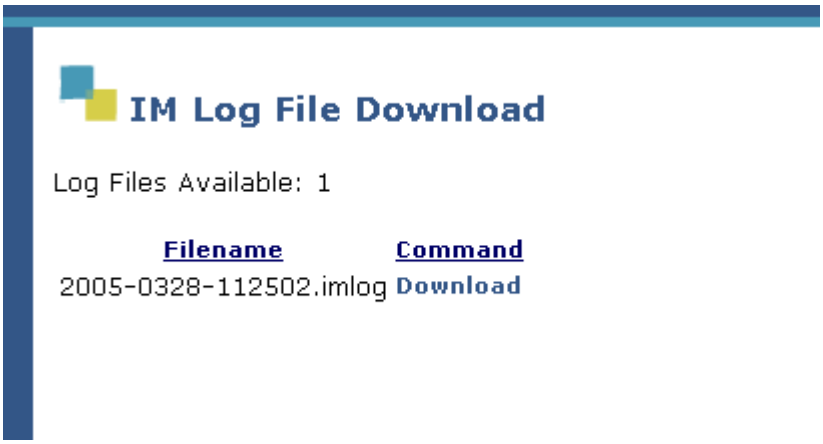
Restart

To stop and then start this service on this host, if it is running. You might select this link if a service appears unresponsive.

IM Logs screen

You may want to download instant messaging log files to your local computer for review or reports.

Figure 88: IM Log File Download screen



IM Logs screen field descriptions

Filename

Each log file is named with its creation date (YYYY-MMDD) and timestamp (HHMMSS). A new file is not automatically created at any specific time or interval, but when the existing file reaches the maximum size for an IM log file, administered in kilobytes (KB) on the IM Log Settings screen on page 332.

IM Logs screen Command

Download

Select **Download** to the right of the log filename you wish to download.

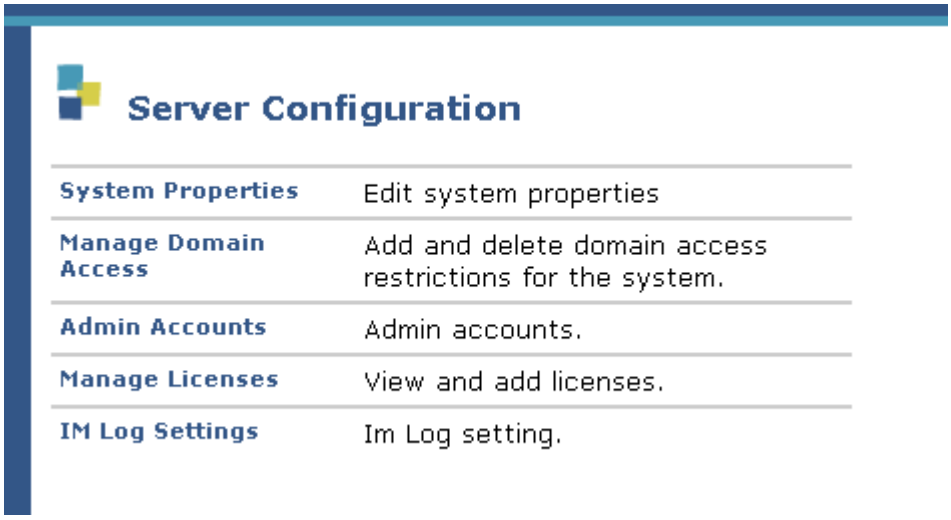
Server Configuration screens

This menu has five selections to administer system properties, domains, administrators, licenses, and logs.

Server Configuration screen menu

This screen provides a menu to easily access the options the menu on the left.

Figure 89: Server Configuration Menu screen



Server Configuration screen field descriptions

System Properties

Select this link to go to the Edit System Properties screen on page 163 and, for example, setup the server's domain.

Manage Domain Access

Select this link to go to the List Domain Access screen on page 319 and view or add another entry in the access list.

Admin Accounts

Select this link to go to the List Administrators screen on page 325 and edit, delete or add a new administrative login account.

Manage Licenses

Select this link to go to the Licenses screen on page 330 and view or add one or more proxy license(s).

IM Log Settings

Select this link to go to the IM Log Settings screen on page 332 and view or set the IM Log or its properties.

Edit System Properties screen

See the Edit System Properties screen on page 163 for the discussion of this topic. There, read about tasks such as how to setup the server's domain.

Domain Access screens

The Domain Access screens allow you to determine the direction, incoming or outgoing, for access in this domain.

You can set access control on the domains that the proxy server is able to access. This access control includes these:

- Incoming and outgoing requests
- Type of control
- Priority of the access

Use this series of screens:

List Domain Access screen on page 319

Add Domain Access screen on page 321

Edit Domain Access screen on page 322

List Domain Access screen

This screen shows the access for the proxy to your SIP domains. From this screen you can add, change, or remove domain access from the proxy.

Figure 90: List Domain Access screen

List Domain Access screen field descriptions

Direction

(Read Only) Shows In, Out, or both for the access direction this entry defines.

SIP Domain

(Read Only) Shows the network name of the domain, traffic for which is defined by this entry.

Action

(Read Only) Shows either Allow or Deny according whether SIP traffic can be routed to, from, or both the domains specified above.

Priority

(Read Only) Shows a whole number representing the relative priority this entry has. The number 1 has highest priority.

Select the **Add Another Entry** link to go to the **Add Domain Access** screen and create a host entry.

List Domain Access screen commands

You may select any of the following links in the Commands column next to a domain access entry.

Edit

Go to the Edit Domain Access screen on page 322 for that entry.

Delete

Delete this domain access entry from the server.

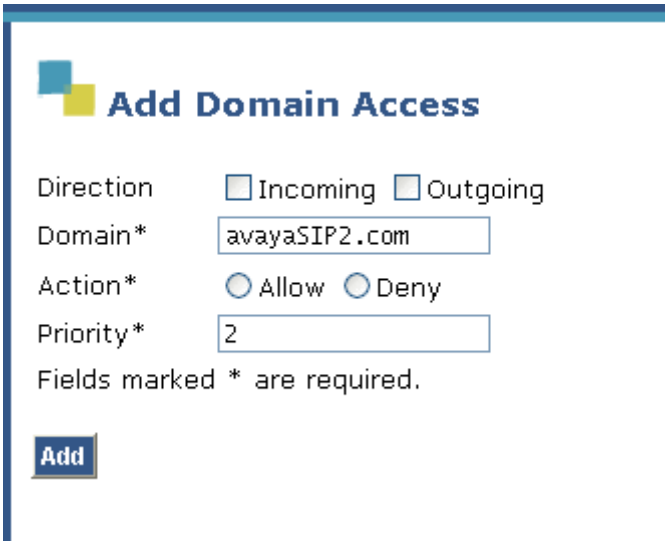
Add Another Entry

If you want to allow the proxy to access more than one domain, select this button.

Add Domain Access screen

Use this screen to add access for the proxy to your SIP domains. With this screen you can set attributes such as incoming or out going calls, set precedence among servers, and allow or deny servers' access.

Figure 91: Add Domain Access screen



Add Domain Access screen field descriptions

Direction

(Required) Select Incoming, Outgoing, or both to specify the access direction this entry is intended to define. Neither is selected for you by default, but to add an entry successfully, you must select a minimum of one direction. You may select both directions.

Domain

(Required) Enter the alphanumeric name of the domain for which traffic is defined by this entry.

Action

(Required) Select either Allow or Deny to specify whether SIP traffic can be routed to, from, or both to and from the domain specified above.

Priority

(Required) Enter a whole number representing the priority this entry has relative to other database entries. The highest priority is 1.

Add Domain Access screen commands

Add

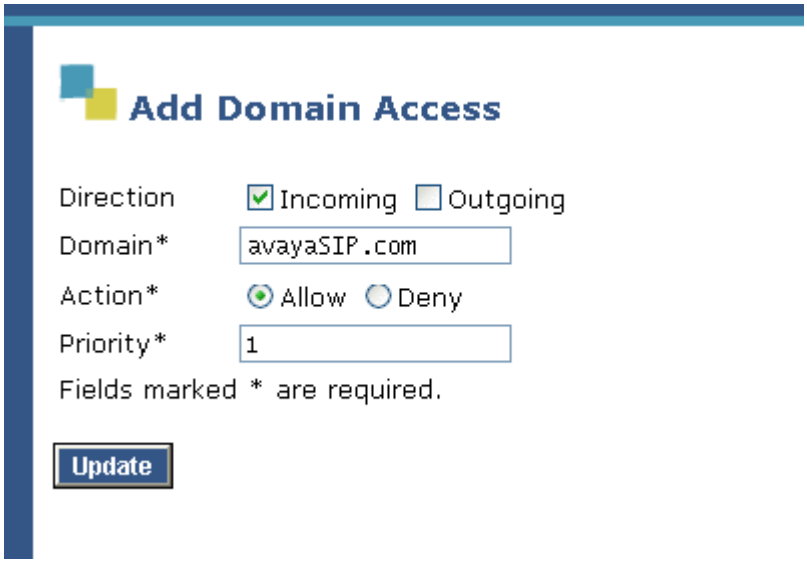
Select Add to submit a domain access entry with the properties you've entered.

Edit Domain Access screen

Make changes to your SIP domain access attributes with this screen.

Even though the title of this screen is Add Domain Access, the Update button at the bottom lets you edit the information presented.

Figure 92: Edit Domain Access screen



Edit Domain Access screen field descriptions

Direction

Select Incoming, Outgoing, or both to specify the access direction this entry is intended to define. Neither is selected for you by default, but to add an entry successfully, you must select a minimum of one direction.

Domain

(Required) Enter the alphanumeric name of the domain for which traffic is to be defined by this entry.

Action

(Required) Select either **Allow** or **Deny** to specify whether SIP traffic can be routed to, from, or both to and from the domain specified.

Priority

(Required) Enter a whole number representing the priority this entry has relative to other database entries. The highest priority is 1.

Edit Domain Access screen commands

Update

Select **Update** to submit a domain access entry with the properties you've entered.

Change Domain procedure

This procedure changes all of the host servers in one domain to another.

On Communication Manager perform these steps:

1. On the ASA, connect to the Communication Manager.
2. Type **`change ip-network-region xx`** command.

   In the above line, *xx* is the ip-network-region number for the SES host to which you want to change.
3. Change the value in the **Authoritative Domain** field to the new domain name.
4. Go through the signaling groups that are associated with the SIP trunks for the SES host to which you want to change its domain name and do the following:
   a. Busy-out the signaling group.
   b. Change the value of the **far-end domain** field to the new domain name.
   c. Release the signaling group.

On the SES host, perform these steps:

1. Launch the Master Administration interface.
2. Navigate to the **System Properties** screen, and change the SIP domain to the new domain name.
3. Select the **Update** button at the end of the page and the **Continue** button on the next page.
4. Select **Update (All)** on the end of the menu on the left and **Continue** on the next page.
5. In the Maintenance interface, navigate to the **Services** screen, stop and start the sipserver, imlogger and eventserver processes.
6. Go to each of the SES home servers and perform these steps:
   a. Navigate to the **Services** web screen, stop and start the sipserver, imlogger and eventserver processes.
   b. On each of the home servers, navigate to the View Registered Users screen.
   c. On the bottom of the Registered Users screen, search for all registered users, select the **Reload-complete** task under **Apply to all registered users on this Home**.
   d. Select **Submit**.
   e. Select **Continue** on the next page to complete sending the notification to the endpoints for reload.

On the Toshiba Business Phone SP-1020A, note this behavior:

- The TSP does not experience call interruption during this procedure.
- TSP automatically re-registers to the home proxy.

Administrator Account screens

Find out the administrators on a system, add one, or change passwords for routine best practices, use these Administrator Account screens:

- List Administrators screen on page 325
- Add Administrator screen on page 327
- Change Administrator Password screen on page 328

List Administrators screen

This screen lets you see the current list of administrators, change their passwords, and add other ones.

Figure 93: List Administrators screen

List Administrators screen field descriptions

Admin Name

(Read Only) Lists the login names of previously administered accounts with administrative rights.

List Administrators screen commands

Change Password

Select the **Change Password** link next to an Admin Name to go to the Change Administrator Password screen on page 328 for that administrator.

Delete

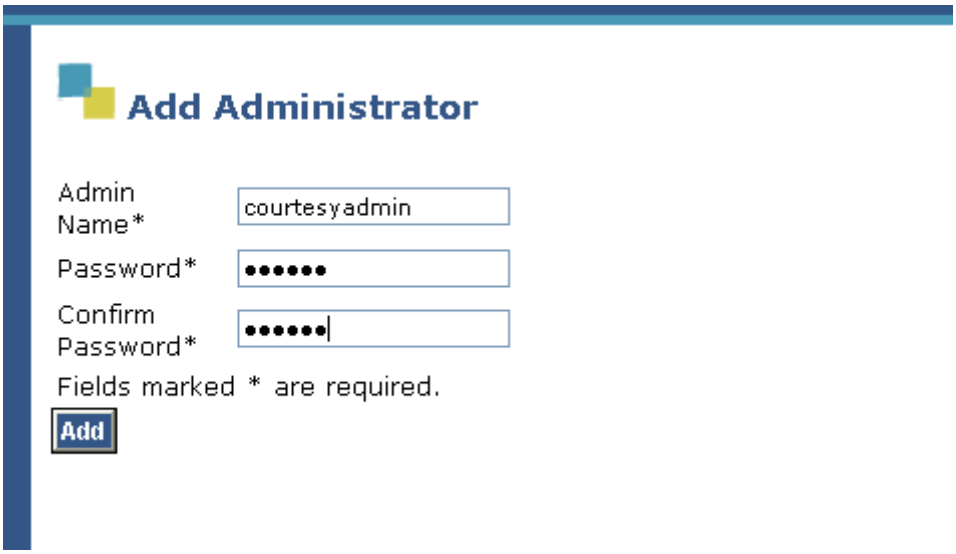
Select **Delete** to delete an administrator account. You cannot delete an administrator account in the list if it is the only one.

Add Another Administrator

Select **Add Another Administrator** to go to the Add Administrator screen on page 327.

Add Administrator screen

Figure 94: Add Administrator screen



Add Administrator screen field descriptions

Admin Name

(Required) Enter a login name for the new administrator, of at least three alphanumeric characters in length.

Password, Confirm Password

(Required) Enter a password of at least 6 and at most 12 alphanumeric characters. Both field entries must match exactly.

Add Administrator screen command

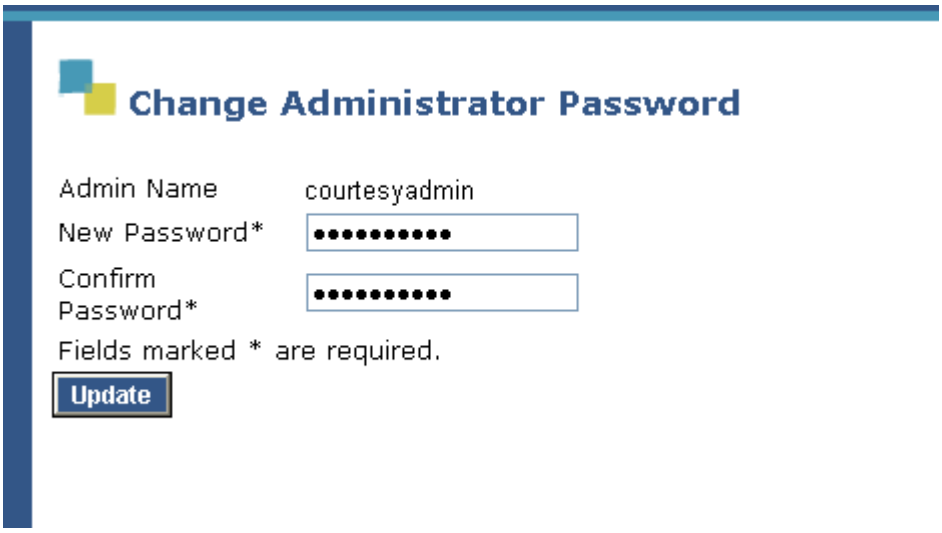
Add

After completing these fields, select **Add** to submit the information to the database on this host.

Change Administrator Password screen

Use this screen to change the password for the administrator for this system.

Figure 95: Change Administrator Password screen



Change Admin Password screen field descriptions

Admin Name

(Read Only) Displays the logon ID of the administrator for whom you are changing the password.

New Password, Confirm Password

(Required) Enter the new password of at least six characters, at least one of which is alphabetic and at least one of which is numeric. Your entries in both of these fields must match exactly. Asterisks will be displayed.

Change Admin Password screen command

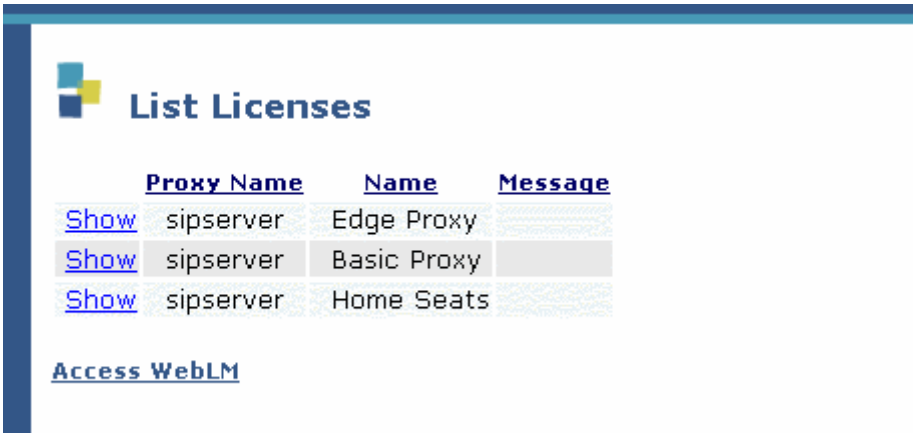
Update

After completing these fields, select **Update** to submit the change to the database.

Licenses screen

If you need to check the licensing on any of the servers use this screen. You may also refer to Server license installation on page 81 for more detail on this topic.

Figure 96: List Licenses screen



Manage Licenses screen field descriptions

Proxy Name

(Read Only) Shows the names for each of the configured proxies authorized on this host.

Name

(Read Only) Shows the names for each of the proxies that are licensed for this Avaya SES server. Duplex server configurations are licensed as one primary host. The licensed proxies include:

- Basic Proxy — each host, whether it be an edge, home, or a combined home/edge server, requires a Basic Proxy license. An edge or combined server also requires an edge proxy license.
- Edge Proxy —there is one edge server, and exactly one edge proxy license, for each SES system.
- Home Seats—Each administered user in the system requires a Home Seat license. Note that licenses are not acquired or released based on user registrations, but rather on administration. So you must not administer more users than you have available Home Seats.

Message

(Read Only) Displays an indicator if there is an issue with acquiring licenses at startup for the proxy software that is running on this server. The possible messages are:

- Blank—if this proxy is configured properly on this host
- Expired—if this proxy is no longer authorized on this host.

Note:

If license(s) cannot be acquired when the proxy server first starts or is restarted, then it will continue to check the specified licensing host (running the WebLM application) for the license(s) every 5 minutes until they are acquired successfully, or until the no-license mode times out. Grace periods for license files may be from 10 to 30 days.

Manage Licenses screen commands

Show

Select **Show** to view the License Information screen. This screen lists the information about the licenses on the server.

Access WebLM

To activate an existing license on this server, select **Access WebLM**. You will start the WebLM application.

The default login/password is now:

Login: admin

Password: See Maestro.

After your first login you will be prompted to change the password. You may at this point change it back to the old password of password if you so desire. WebLM will then log you out and expect you to log back in with your new password.

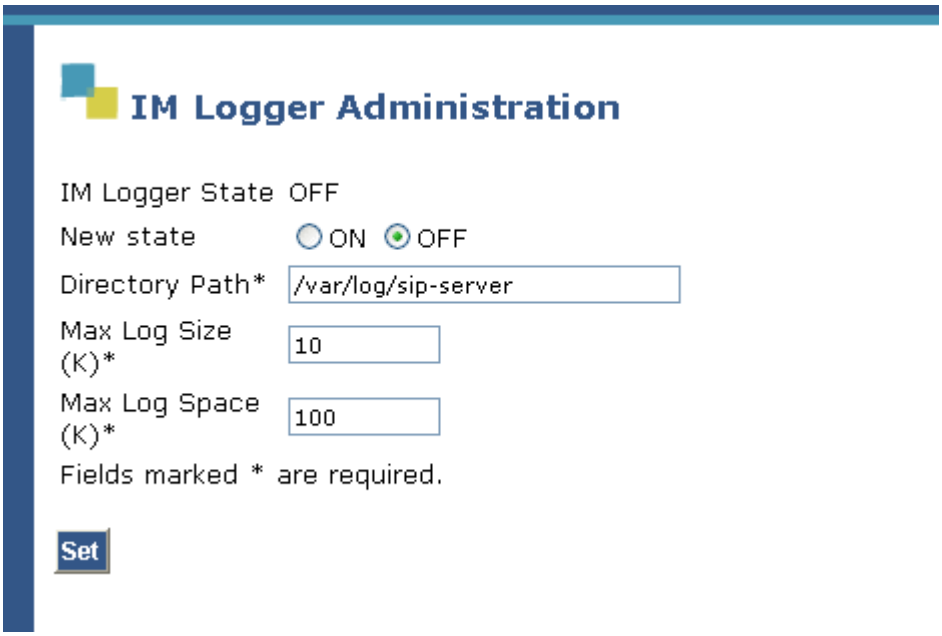
IM Log Settings screen

Tip:

The following tips will help you administer the IM Logger service:

- A new IM Log file is created whenever IM Logger starts.
- This file logs instant messages until it reaches the maximum size for an IM log file, administered in kilobytes (K bytes). See IM Logs screen on page 316.
- A record is placed in the log file whenever logging is enabled and disabled from this administration screen.
- The maximum log space administered (also in K byte) must be higher than the maximum log file size.
- Each log file name includes the date and timestamp of when that file was created. Note that a new file is not automatically created at any specific time or interval.
- The default values for Max Log Size and Max Log Space are 10K bytes and 100K bytes respectively, which are designed to be appropriate for lightly loaded instant-messaging systems, and should be adjusted according to a customer's IM volume.

Figure 97: IM Logger Administration screen



IM Log Settings screen field descriptions

IM Logger State

(Read Only) This field shows the current state of the IM Logger service as OFF or ON. If this field is set as OFF, the system creates no log files.

New State

Select the state you want to set the IM Logger as ON or OFF. By default, the current state is selected. By default, a new IM log file is created whenever IM Logger starts.

Directory Path

(Required) Enter a full path name to the directory to where the IM logger files should go. By default, the value of the path entered for you is /var/log/sip-server.

Max Log Size (K)

(Required) Enter a whole number of kilobytes as the maximum size you want to allow for each IM log file. The default value is 10 KB, which is 0.1 of the maximum log space specified by default. You can change this ratio of logs to available space, so long as the number entered here is smaller that the number entered in the **Max Log Space** field, described below.

Max Log Space (K)

(Required) Enter a whole number of kilobytes as the maximum space you want to allow for all log files, The default value is 100 KB, or approximately 10 of the maximum sized IM log files specified by default.

You can change this ratio, as long as the number here is larger that the number for the **Max Log Size** field, described above.

IM Log Settings screen command

Set

Enter the properties for IM Logger and select **Set** to submit your changes to this server.

Chapter 9: Maintenance Web Interface

This section describes in detail the use and meaning of the screens in the Maintenance interface.

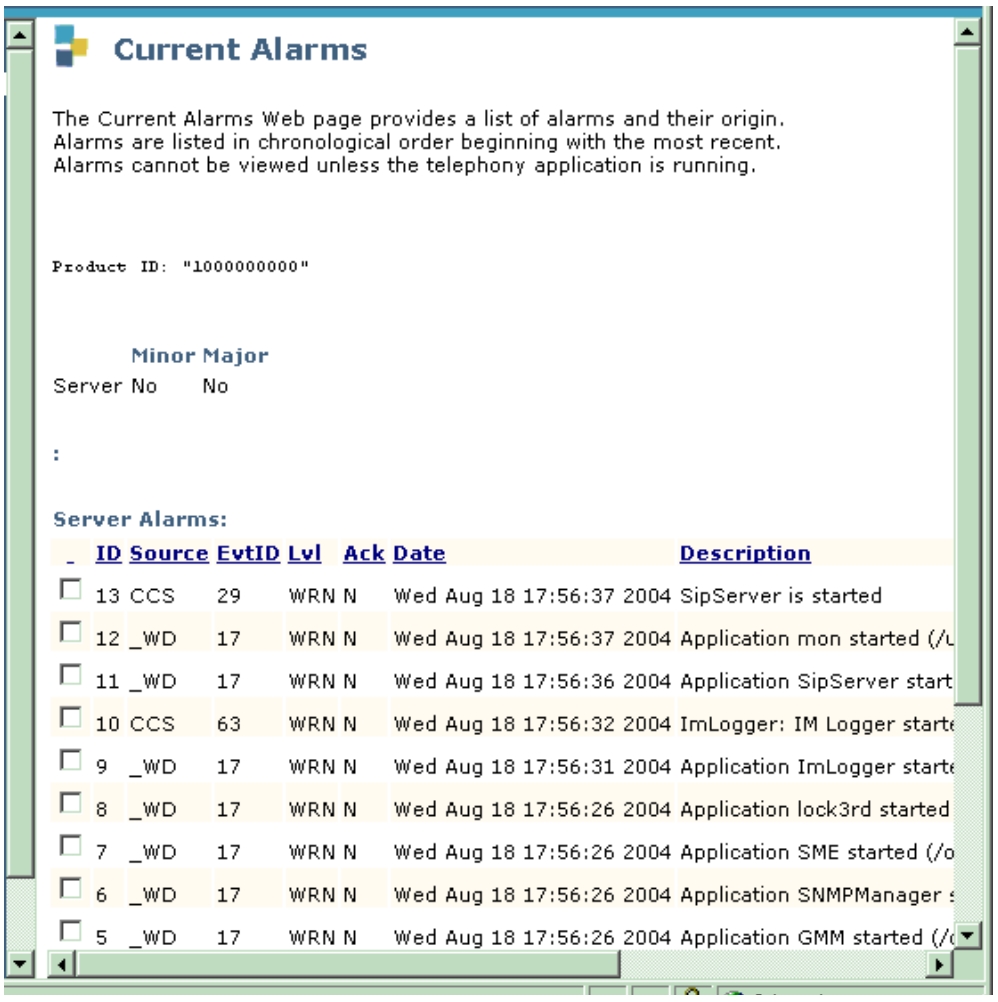
Alarms screens

Alarm screens are these:

A helpful adjunct to these alarm screens are the Diagnostics screens on page 341.

Current Alarms screen

Figure 98: Current Alarms screen



Current Alarms screen field descriptions

Use the Current Alarms page to view a list of outstanding alarms. This page shows either a summary of alarms, if present, or a message stating that no alarms are present.

Product ID

Use these steps to view current alarms against the server identified by this Product ID:

1. Check if any alarms are present. If no alarms appear, continue with your web-administration activities. If yes, continue.
2. If alarms are present, the bottom part of the page shows a detailed list of outstanding alarms:

ID

This is a unique identification number assigned to the alarm.

Source

This is the abbreviated name of the software process that generated a platform alarm, as follows:

- **ENV** for environment attributes on the motherboard such as temperature, voltage, fan
- **FSY** for file synchronization
- **GAM** for global alarm manager
- **GMM** for global maintenance manager
- **KRN** for kernel
- **LIC** for license server
- **logon** for logon attempts
- **NIC** for Ethernet network interface
- **SME** for server maintenance engine
- **TLG** for trace log
- **UPS** for uninterruptible power supply
- **USB** for universal serial bus
- **_WD** for watchdog

EvtID

The event identification number for each alarm is used to identify a particular event from a given source that generated the alarm.

Lvl

The level of the alarm is minor, major, or warning.

Ack

Displays a Y (yes) or N (no) to indicate whether the alarm has been acknowledged by the Initialization and Administration System (INADS).

Date

This is the timestamp assigned to the alarm when it occurred.

Description

The Description field provides a brief explanation of the alarm.

Server Alarms

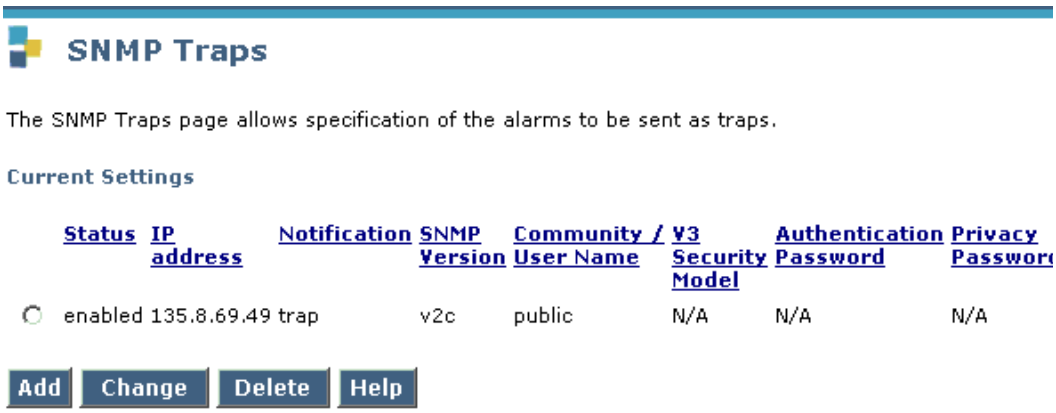
The Current Alarms page allows you to clear (remove) some or all of the displayed alarms.

CAUTION:
Clearing alarms only removes the alarm notifications from the active alarm list. It does *not* remove the conditions that caused the alarms.

1. Select one or more alarm entries. select **Clear**. All checked items disappear from the active alarm list. You will not receive a response if an entry is not selected before clicking **Clear**.
2. To remove all alarm entries from the list, select **Clear All**.

SNMP Traps screen

Figure 99: SNMP Traps screen



SNMP Traps screen field descriptions

Use the **Configure** page to configure destinations for SNMP traps or informs (alarms and notable events) on the corporate network. Some form of corporate network management system (NMS) must be in place to collect the SNMP messages. In addition, the SNMP ports must be enabled on the Ethernet interface to the corporate LAN. Note that the CCS-AVAYA MIB is located in the `/var/home/ftp/pub/mib` directory.

Status

Shows if the configured destination is enabled or disabled.

- Traps or inform requests (informs) are only sent to a destination if enabled.
- Disabling a destination keeps the configuration data in the file, but stops traps and informs from being sent.

IP Address

Every computer that communicates over the Internet is assigned an IP address that uniquely identifies the device and distinguishes it from other computers on the Internet. An IP address consists of 32 bits, often shown as 4 octets of numbers from 0-255 represented in decimal form instead of binary form.

Notification

Refers to traps or inform requests as described above.

SNMP Version

The three final fields on this page are blank if SNMP Version 1 or Version 2c are used.

Community or User Name

The authentication mechanism used by the different SNMP versions.

- Community Name Authentication is a plain text string used for SNMP v1 and v2c.
- User Name is part of the user-based security model for SNMP v3. This character string indicates the user who is authorized to send traps to the destination.

V3 Security Model

The level of security to use when sending v3 traps. Options are None, Authentication, and Privacy.

Authentication Password (v3 only)

Pass phrase for the user specified in the User Name field, used to digitally sign or sanction v3 traps.

Privacy Password (v3 only)

Pass phrase for the user specified in the User Name field, used to encrypt v3 traps.

Select **Add** for a new trap destination, **Change** to modify the trap destination, or **Delete** to remove the trap destination.

The SNMP Trap page may display the following error:

Unable to contact alarm agent: The Trap Destinations page was unable to notify the server's alarm agent that the configuration file was changed. This error could occur following any add, change, or delete operation.

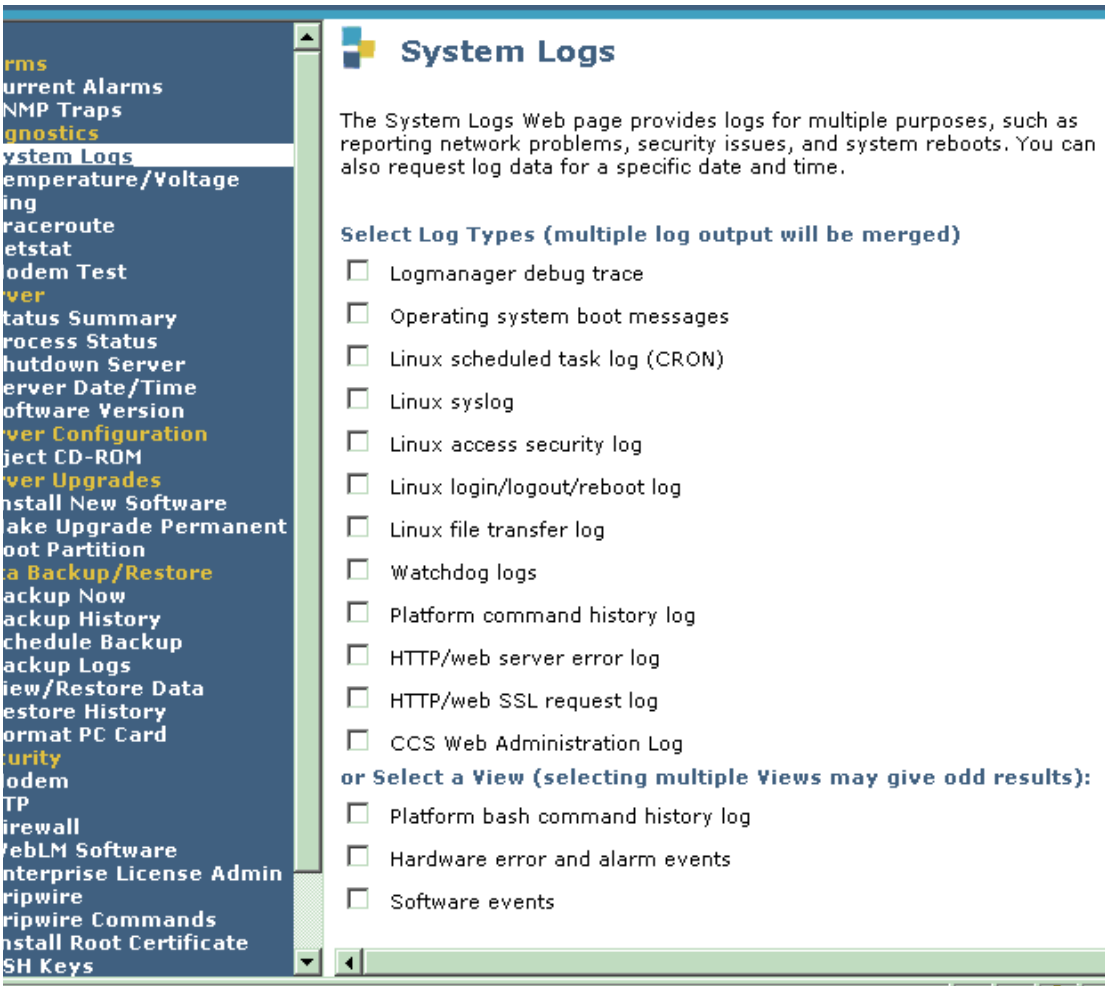
Diagnostics screens

- System Logs screen
- Temperature/Voltage screen
- Ping screen
- Traceroute screen
- Netstat screen
- Netstat results screen

System Logs screen

This page enables you to select and view system log entries for a period of time you specify. You can use this page to view detailed information about network problems, security issues, system reboots, mail, and so on.

Figure 100: System Logs screen



System Logs screen field descriptions

Select Log Types (multiple log output will be merged)

Select one log type at a time. If you select more than one, the log files merge.

Log Type	Description
lm	**Log Manager Debug Trace** (default): Provides information about SES hosts and High Availability Platform software such as restarts, initializations, and shutdowns, duplication status, process errors, system alarms, and communication with external gateways and port networks. The log rolls over when it reaches its size limit.
lxboot	**Linux boot messages**.
lxcron	**Linux Scheduled Task log (CRON)**. Shows information from the Linux scheduling daemon.
lxsys	**Linux Syslog**. Collects all the system messages produced by the various subsystems (processes) running on Linux.
lxsec	**Linux Access Security log**. Information pertaining to logon connections to the Linux system. Actions logged in this file include opening or closing a telnet session and modem messages.
lxwtmp	**Linux login/logout/reboot log**. Information about Linux logon and logout procedures, as well as system reboots.
lxxfer	**Linux File Transfer log**. Contains information about files copied to or retrieved from the system. It indicates, among other things, the time, user, and files that were copied to or retrieved from the system.
wd	**Watchdog Logs**. Only the watchdog process writes to this log. It contains information about application starts, restarts, failures, shutdowns, heart beating, and Linux reboots. It also contains information about processes that use excessive CPU cycles.
cmds	**Platform Command History Log**. High Availability Platform commands are logged to this file. These are the commands that modify the server administration or status. For all the shell commands executed on the system see the lxsys log or the bashhist view.

Log Type	Description
httperr	**HTTP/web server error log**. These are errors and events generated by the platform web server and include items like web server restart, abnormal CGI script file terminations, and certificate mismatches.
httpssl	**HTTP/web secure sockets layer (SSL) request log**. These are all the requests made of the web servers SSL module. All pages requested or placed in secure mode are indicated.
ccsadmin	SES server **Web Administration log**. The last 16 administrative functions performed are in this log.

Select a View (selecting multiple Views may give odd results)

Select one view only. If you select more than one, the Views may merge. You can define views in the log view* files, however, the following are included:

View	Description
bashhist	**Platform bash command history log**. The list of commands run by interactive bash shells are these fields: PPID: process ID of the parent shell. PID: process ID of the shell. UID: user ID under which the shell is executing. Zero (0) means root or super user.
hwerr	**Hardware error and alarm events**. The events that go into the SES hardware error and alarm logs.
swerr	**Software events**. The events that go into the SES server's software error log.

Select Event Range

Select one of the following event ranges:

1. Event ranges:
   - Today
   - Yesterday
   - View entries for this date and time. Complete the year, month, day, hour, and minute text boxes as desired to focus your search.
2. Enter a 4-digit year, and 2-digit entries for the other fields as indicated.
3. You cannot skip fields (such as specifying a year and day but not month).

Note:

The more information you enter, the more specific your search becomes. For example, to view all events for March 2002, enter 2002 for the year and 03 for the month. To view only the events for March 27, 2002, also enter 27 for the day, and so on.

Match Pattern

(Optional) To further limit your search, enter a keyword in the Match pattern field (such as a name or message type). The log will display only those entries that contain this keyword. You must check the box to the left of this field to search for entries with this keyword.

Display Format

You can view up to 200 lines of text on a Web page. Type the number of lines you want to view at one time.

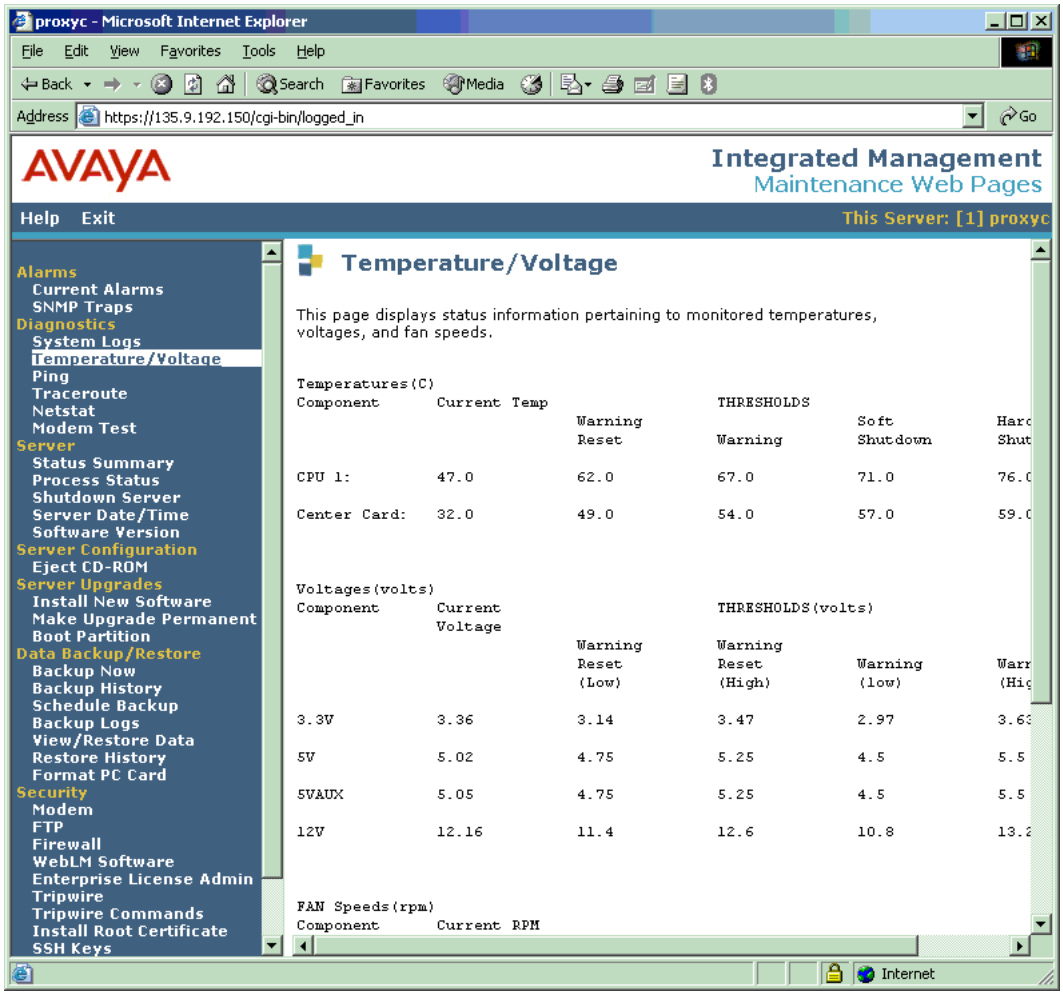
Select **View Log** to submit the requested information on this host.

Temperature/Voltage screen

The Temperature/Voltage screens are different for the S8500 and S8500B hardware. Check in these sections for the information you need.

- Temperature/Voltage screen on S8500 on page 346
- Temperature/Voltage screen on S8500B on page 349

Figure 101: Temperature/Voltage screen on S8500



Temperature/Voltage screen field descriptions S8500

Use this page to view temperature, fan speeds, and voltage information about the server. You can quickly assess whether or not the hardware components are performing within normal ranges. If alarm conditions exist, you can take corrective action.

Temperatures (C degrees Celsius)

Component: the device being monitored in temperature degrees.

Current Temperature: a current temperature value is indicated.

Thresholds: If the temperature range is between warning reset and warning, it is considered normal (that is, between 10.00 and 50.00 degrees Celsius).

- **Warning Reset**: When this threshold for components is set, and the temperature drops to a value below the Warning Reset value, the server or ASM processor assumes the Reset setting and returns to normal. No additional alarms are generated.
- **Warning**: When the temperature of a component exceeds the setting for the Warning threshold, an alert notifies users. The same alert message is sent to INET. When the condition stabilizes, no additional messages are sent.
- **Soft Shutdown**: When the temperature exceeds the soft shutdown setting, users are alerted that the RSA card communicates a shut down to the system.
- **Hard Shutdown**: When the temperature exceeds the Hard Shutdown setting, the system shuts down.

CAUTION:

If the temperature exceeds 50 degrees Celsius, you must adjust the room air conditioning or power off the server until the condition is corrected. To distinguish the particular condition that caused an alarm, go to the System Logs screen and view the Linux system log (syslog) file to see the message that corresponds with the condition.

Voltages (volts)

For each component, its current temp is followed by critical low, warning low, warning high, and critical high thresholds. If the temperature is in the range between warning low and warning high thresholds, it is considered normal (that is, between 10.00 and 50.00 degrees Celsius).

Component: device being monitored in volts.

Current Voltage: current value of the component is indicated

Threshold: Thresholds are identified by warning reset (low), warning reset (high), warning (low), and warning (high). If the CPU I/O voltage causes a critical low alarm, the log file shows a similar entry: *CPU I/O Voltage reached Critical Low. Value = xxxx*.

- **CPU IO**. The value for CPU IO voltage should be between the critical low and critical high thresholds.
- **CPU Core**. The value for CPU core voltage should be between the critical low and critical high thresholds shown on this page.
- **3.3V**. The value for the 3.3V power supply on the motherboard should be between the critical low and critical high thresholds.
- **5V**. The value for the 5V power supply on the motherboard should be between the critical low and critical high thresholds.
- **+12V**. The value for the +12V power supply on the motherboard should be between the critical low and critical high thresholds.
- **-12V**. The value for the -12V power supply on the motherboard should be between the critical low and critical high thresholds.

Fan Speeds (rpm)

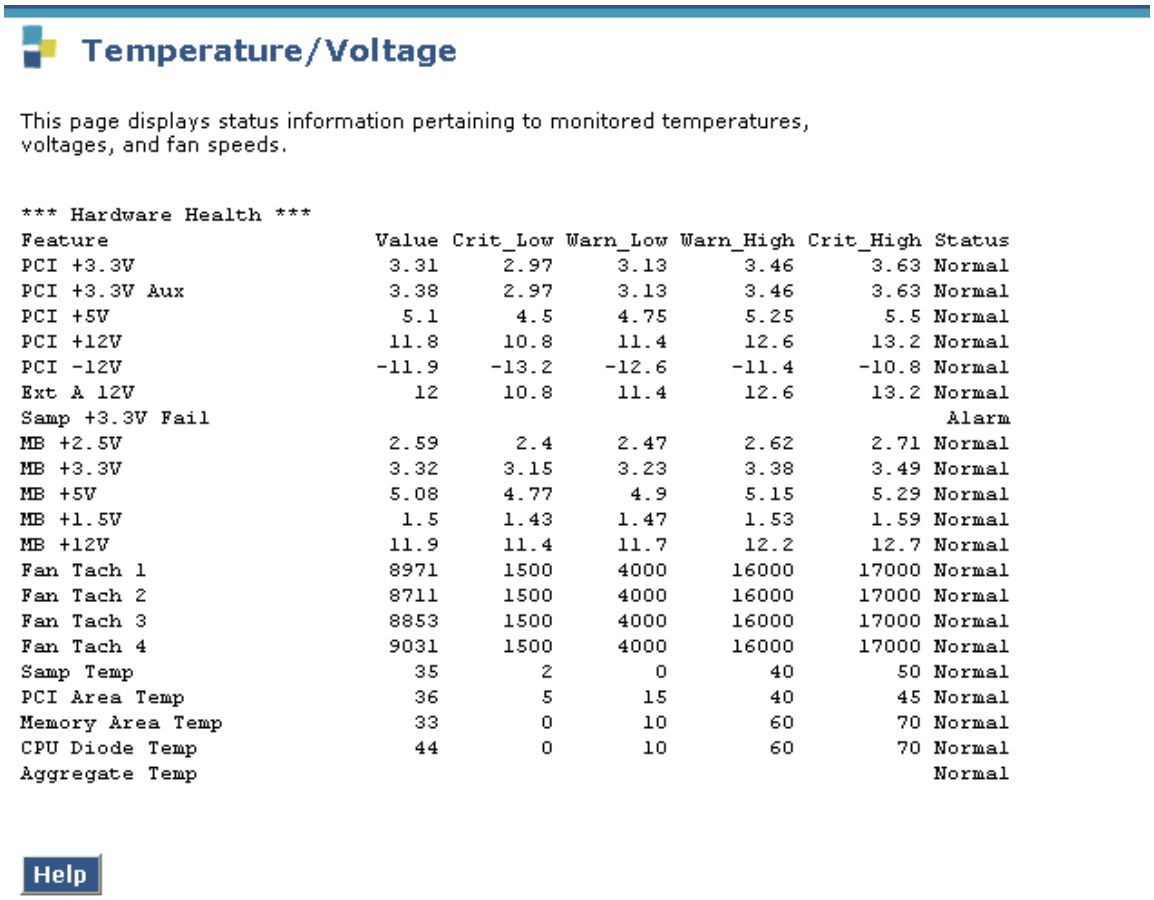
Component. Number of fans are listed.

Current RPM. The server motherboard has several fans, each of which has two thresholds, a critical low RPM and a warning low RPM. For each fan, the value should be between 6278 and 6600 RPMs. When all the fans run at a speed below the values mentioned, the system generates an All Fan Failure alarm. In this case, you should physically check each fan to verify it is running slower than specified.

ECC RAM

The currently installed RAM size and type for each installation bank, as well as the total RAM amount.

Figure 102: Temperature/Voltage screen on S8500B



Temperature/Voltage

This page displays status information pertaining to monitored temperatures, voltages, and fan speeds.

*** Hardware Health ***

Feature	Value	Crit_Low	Warn_Low	Warn_High	Crit_High	Status
PCI +3.3V	3.31	2.97	3.13	3.46	3.63	Normal
PCI +3.3V Aux	3.38	2.97	3.13	3.46	3.63	Normal
PCI +5V	5.1	4.5	4.75	5.25	5.5	Normal
PCI +12V	11.8	10.8	11.4	12.6	13.2	Normal
PCI -12V	-11.9	-13.2	-12.6	-11.4	-10.8	Normal
Ext A 12V	12	10.8	11.4	12.6	13.2	Normal
Samp +3.3V Fail						Alarm
MB +2.5V	2.59	2.4	2.47	2.62	2.71	Normal
MB +3.3V	3.32	3.15	3.23	3.38	3.49	Normal
MB +5V	5.08	4.77	4.9	5.15	5.29	Normal
MB +1.5V	1.5	1.43	1.47	1.53	1.59	Normal
MB +12V	11.9	11.4	11.7	12.2	12.7	Normal
Fan Tach 1	8971	1500	4000	16000	17000	Normal
Fan Tach 2	8711	1500	4000	16000	17000	Normal
Fan Tach 3	8853	1500	4000	16000	17000	Normal
Fan Tach 4	9031	1500	4000	16000	17000	Normal
Samp Temp	35	2	0	40	50	Normal
PCI Area Temp	36	5	15	40	45	Normal
Memory Area Temp	33	0	10	60	70	Normal
CPU Diode Temp	44	0	10	60	70	Normal
Aggregate Temp						Normal

Help

Temperature/Voltage screen field descriptions

Use this page to view temperature, fan speeds, and voltage information about the server. You can quickly assess whether or not the hardware components are performing within normal ranges. If alarm conditions exist, you can take corrective action.

Feature

The Feature column lists the elements being measured.

- PCI card voltages
- EXT A card voltage
- Sample failure and alarm

- Motherboard (MB) voltages of power supply
- Fan speeds as measured by tachometer
- Temperatures of various areas on the motherboard.

CAUTION:

If the temperature exceeds 50 degrees Celsius, you must adjust the room air conditioning or power off the server until the condition is corrected. To distinguish the particular condition caused an alarm, go to the System Logs screen on page 342 and view the Linux system log (syslog) file to see the message that corresponds with the condition.

The row **Samp Temp** shows the temperatures used to determine if the actual temperature reading is high or low.

Value

The current reading of the component being measured.

Crit_Low

The excessively low value at which at which a major alarm is generated.

Warn_Low

The somewhat low value at which a warning alarm is generated.

Warn_High

The moderately high value at which at which a major alarm is generated.

Crit_High

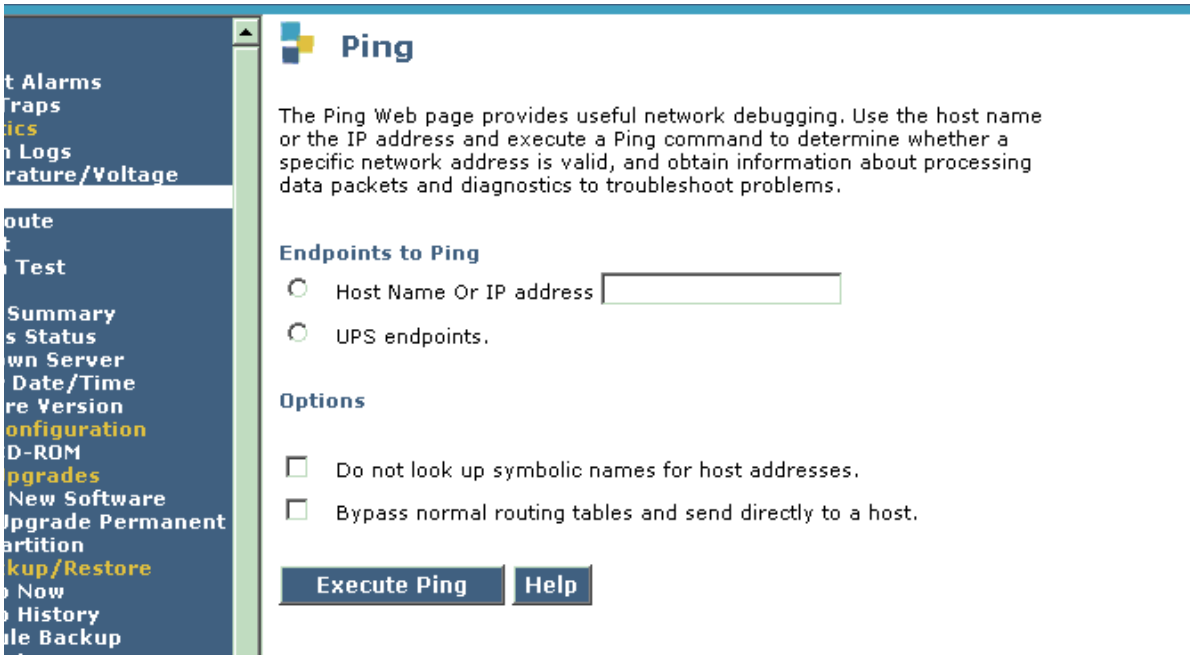
The excessively high value at which at which a major alarm is generated.

Status

A generalization stating that the reading is either within normal limits or not.

Ping screen

Figure 103: Ping screen



Ping screen field descriptions

Use the Ping page to execute the ping command for information about your network. Typically, use the ping command to:

- Test whether or not a specified address in your network is working.
- Obtain information about how quickly and efficiently your network is processing data packets.
- Use the diagnostic information available through the command to manage your network.

Host Name Or IP address

Enter or select the host name or IP address you want to ping.

UPS Endpoints

Select this option to ping all Uninterruptible Power Supply (UPS) endpoints.

Options

Do not look up symbolic names for host addresses. Select this option to ping by IP address. If you do not select this option, the system looks up symbolic names for the host addresses. To do so, the system uses the domain name server, which translates the IP address to a symbolic name. If the domain name server is unavailable, the ping will not be successful.

Bypass normal routing tables and send directly to a host. Select this option to ping a local host on an attached network. That is, select this option to bypass the routing table and ping a local host through an interface that has no route through it. If the host is not on a network that is directly attached, the ping will be unsuccessful and you will receive an error message.

Execute Ping

Start your **`ping`** command. If the ping is successful, the **Execute Ping** results page displays a brief summary that shows the number of packets sent and received. The summary also shows the minimum, average, and maximum of the round-trip times.

Ping results screen

When you run the ping command, a results page shows whether the command was successful or not. The following sections describe successful and unsuccessful ping results.

Successful ping results

If the ping command runs successfully, the Execute Ping results page displays a brief summary that looks something like this:

```
PING www.asite.com (135.9.4.93) from 135.9.77.30: 56 (84) bytes of data.
64 bytes from www.asite.com (135.9.4.93): icmp_seq=0 ttl=245 time=6.3 ms
64 bytes from www.asite.com (135.9.4.93): icmp_seq-1 ttl=245 time=6.3 ms
--- www.asite.com ping statistics ---
2 packets transmitted, 2 packets received, 0% loss
round-trip min/avg/max = 0.3/3.3/6.3 ms
```

Unsuccessful ping results

If the ping command does not run successfully, the Execute Ping results page displays an error message. Each error message points to one or more possible problems, as follows:

100% packet loss. This error message can indicate a variety of things, including:

- The network host is down.
- The host is denying the packets.
- The network is down.
- The ping was sent to the wrong address.

Packets are rejected. This message indicates that the host is rejecting the packets.

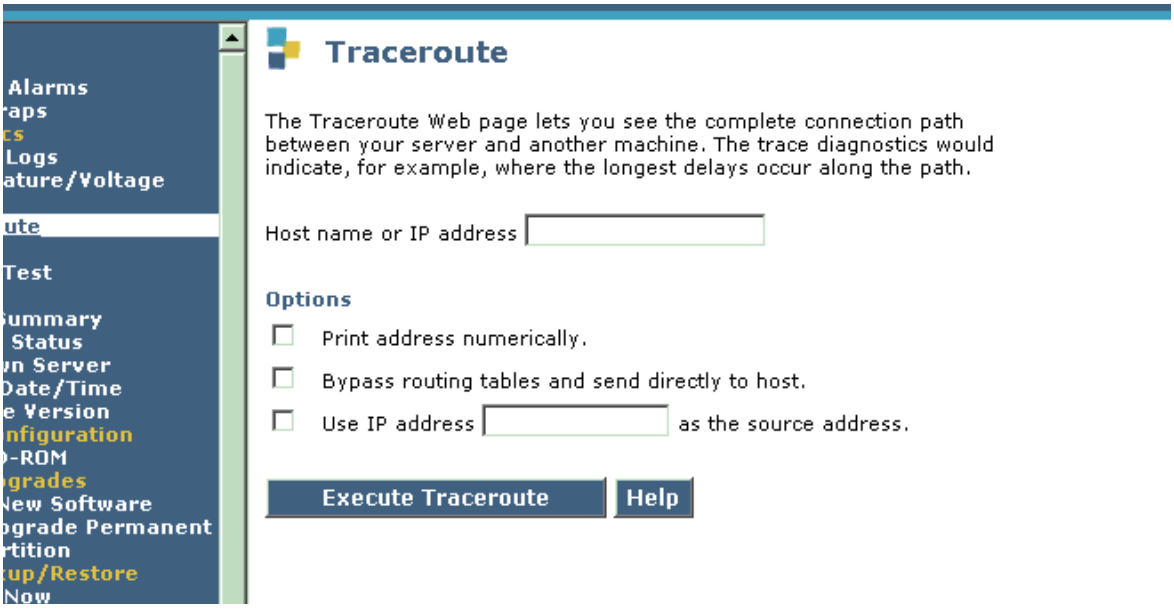
Packets did not reach the host. This message indicates there is a problem with the network so that the ping packets cannot reach the host.

Traceroute screen

Use this page to see the full connection path between your site and another network address. The traceroute command tracks how IP packets move through the gateways connecting the Avaya server network hardware. The traceroute command does this by launching probe packets with a small time to live and then listening for an Internet Control Message Protocol (ICMP) Time Exceeded reply from a gateway.

You can use the traceroute command to evaluate the hops taken between the links in your TCP/IP network. Hops are the short, individual trips that packets take from one router to another on the way to their destinations.

Figure 104: Traceroute screen



Traceroute screen field descriptions

Host Name or IP Address

(Required) Enter the destination host name or IP address.

Options

Print address numerically.

Select this option to print the hop addresses numerically rather than by symbolic name and number. If you do not select this option, the system looks up symbolic names for the host addresses. To do so, the system uses the domain name server, which translates the IP address to a symbolic name. If the domain name server is unavailable, the traceroute command will be unsuccessful.

Bypass routing tables and send directly to host.

Select this option to run the traceroute to a local host through an interface that has no route through it. That is, select this option to run the traceroute to a local host on an attached network.

If the host is not on a network that is directly attached, the traceroute will be unsuccessful and you will receive an error message.

Use IP address as the source address.

This option lets you specify an alternate IP address as the source address. Doing so enables you to force the source address to be something other than the IP address of the interface from which the probe packet was sent.

Click **Execute Traceroute**.

Traceroute results screen

When you run the traceroute command, the Execute Traceroute results page shows whether the command was successful or not. The following sections describe successful and unsuccessful traceroute results.

Successful traceroute results

If the traceroute command runs successfully, the Execute Traceroute results page displays a summary that looks something like this:

traceroute to server.mycompany.com (192.168.1.126), 30 hops max, 38 byte packets

1 server1.mycompany.com (192.168.1.254) 0.324 ms 0.226 ms 0.206 ms

2 server2.mycompany.com (192.168.2.254) 0.446 ms 0.372 ms 0.288 ms

3 server.mycompany.com (192.168.1.126) 0.321 ms 0.227 ms 0.212 ms

As shown in the example given above, the traceroute output in the first line differs from the output in subsequent lines. The following two sections describe the traceroute output.

First line of output

The first line of traceroute output describes the parameters within which the command was run. It shows:

- Destination host name and IP address (server.mycompany.com (192.168.1.126))
- Maximum number of hops (30 hops max)
- Packet size (38 byte packets)

Subsequent lines of output

The subsequent lines of traceroute output describe each hop completed for the traceroute. These lines show:

- Hop number (1, 2, and 3)
- Address of the gateway computer, which is the host name, followed by the IP address. For example, server.mycompany.com (192.168.1.254).

If you elected to print the addresses numerically, no host name appears in the output. For example:

1 192.168.1.254 0.778 ms 0.590 ms 0.216 ms

2 192.168.2.254 0.507 ms 0.449 ms 0.311 ms

- Round-trip time to the gateway computer (for example, 0.324 ms 0.226 ms 0.206 ms)

Note:

Note that each hop is measured three times. If you see an asterisk (*) in the round-trip time part of the output, it indicates that a hop has exceeded some limit.

Unsuccessful traceroute results

If the traceroute command does not run successfully, the Execute Traceroute results page displays information about the error, as follows:

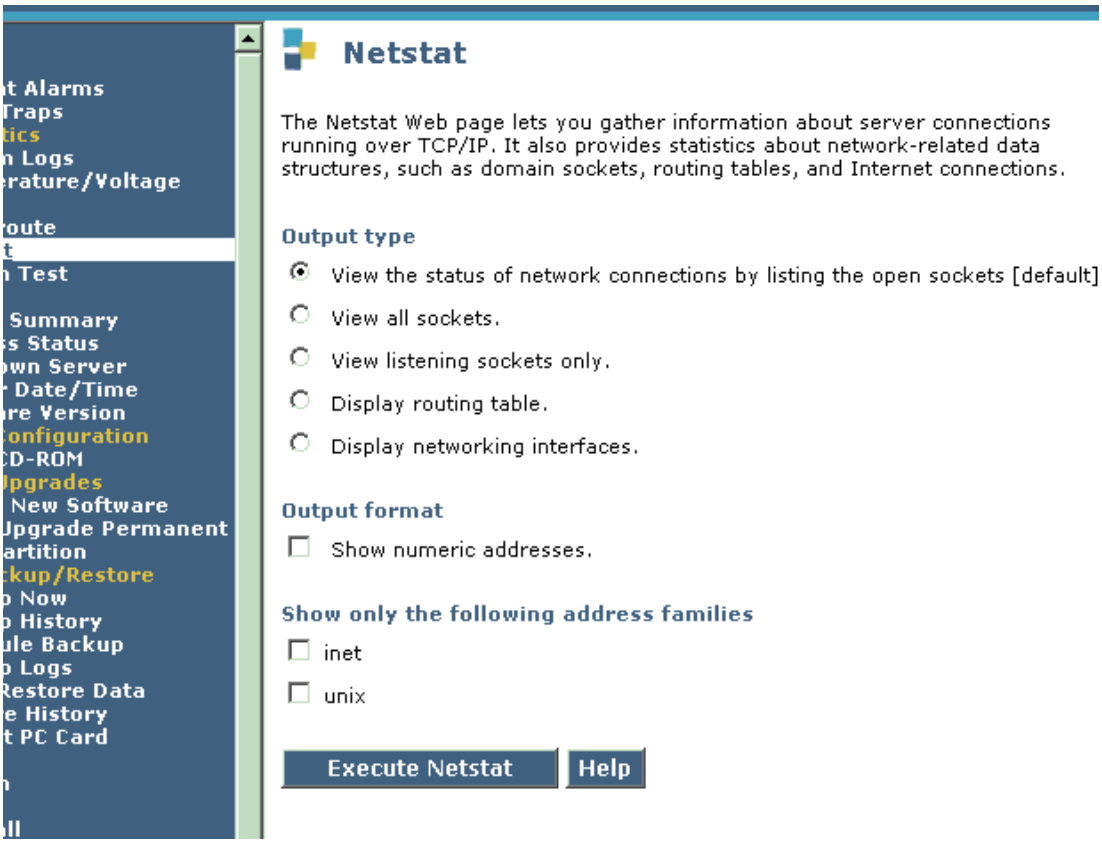
- traceroute: unknown host www.unknown.com
- This is because the host www.unknown.com cannot be reached.

If you see an asterisk (*) in the round-trip time part of the output, it indicates that a hop has exceeded some limit.

Netstat screen

Use this Netstat page to obtain information about server connections running over TCP/IP. The netstat command provides statistics about the following network-related data structures: domain sockets routing tables, and Internet connections.

Figure 105: Netstat screen



Netstat screen field descriptions

Output type

View the status of network connections by listing the open sockets. Choose this default selection to view the active Internet connections, except those associated with the server processes.

View all sockets. Choose this selection to view the state of all domain sockets, including those used by server processes.

View listening sockets only. Choose this selection to view only those active domain sockets that are used by server processes.

Display routing table. Choose this selection to view the routing table for specific IP addresses.

Display networking interfaces. Choose this selection to view the kernel interface table, which provides information about the packet traffic on the network interfaces.

Output format

To ensure that the addresses display numerically on the results page, click **Show Numeric Addresses.**

CAUTION:

If you do not select this option, the system searches for symbolic names for the addresses using the domain name server. If the domain name server is unavailable, the netstat command will be unsuccessful.

Show only the following output families

- **inet** Select this option to limit the statistics or address control block reports to inet addresses. The socket type is AF_INET.
- **UNIX** Select this option to limit the statistics or address control block reports to unix addresses. The socket type is AF_UNIX, that is, local machine socket.

Note:

To view results for inet and unix address families on the same page, select both options.

Click **Execute Netstat**.

Netstat results screen

The information displayed in the Netstat results page depends on your output type selection using the Execute Netstat command. The sample results below combine output for inet and UNIX address families, and may not be applicable to each output type selection.

Active Internet connections (w/o servers)

State Local Send- Recv- Proto Foreign PID/Program
Address Q Q Address name

831/ Established Srv2.:2402 tcp 0 mycom- 0

srv1:www

Established Srv3:1077 tcp 0 mycom- 0 1969/

srv1:telnet

Established Srv3:1076 tcp 0 mycom- 0

srv1:telnet

Active UNIX domain sockets (w/o servers)

Path State Type Flags RefCnt Proto lNode

/dev/log 33148 DGRAM [ ] unix 7

42350 DGRAM [ ] unix 0

38530 DGRAM [ ] unix 0

The sample result given above shows output for both inet and unix address families. The following sections describe the two types of output.

Output for inet address families

Proto is the protocol used by the socket.

Recv-Q is the number of bytes not copied by the user program connected to the socket.

Send-Q is the number of bytes not acknowledged by the remote host.

Local Address is the host name of the socket.

Foreign Address is the remote host name and port number of the socket.

State is the state of the socket. The state might have one of the following values:

ESTABLISHED. The socket has established a connection.

SYN_SENT. The socket is actively attempting to establish a connection.

SYN_RECV. The socket has received a connection request from the network.

FIN_WAIT1. The socket is closed, and the connection is shutting down.

FIN_WAIT2. The connection is closed, and the socket is waiting for a shutdown from the remote end.

TIME_WAIT. The socket is waiting after being closed to handle packets still in the network.

CLOSED. The socket is not being used.

CLOSE_WAIT. The remote end has shut down, and it is waiting for the socket to close.

LAST_ACK. The remote end has shut down, and the socket is closed. The socket is waiting for acknowledgment.

LISTEN. The socket is listening for incoming connections.

CLOSING. Both local and remote sockets are shut down, but all the data are still not sent.

UNKNOWN. The state of the socket is unknown.

Output for unix address families

Proto is the protocol used by the socket.

RefCnt is the reference count of processes attached via this socket.

Flags is used for unconnected sockets if their corresponding processes are waiting for a connect request

Type is the type of socket access, as follows:

SOCK_DGRAM. The socket is used in Datagram mode (without connections).

SOCK_STREAM. The socket is a stream socket.

SOCK_RAW. The socket is used as a raw socket.

SOCK_RDM. The socket serves reliably delivered messages.

SOCK_SEQPACKET. The socket is a sequential packet socket.

SOCK_PACKET RAW. The socket is an interface access socket.

UNKNOWN. The socket is unknown.

State is the state of the socket. For a list of possible socket states, see the description for Output for inet address families on page 359.

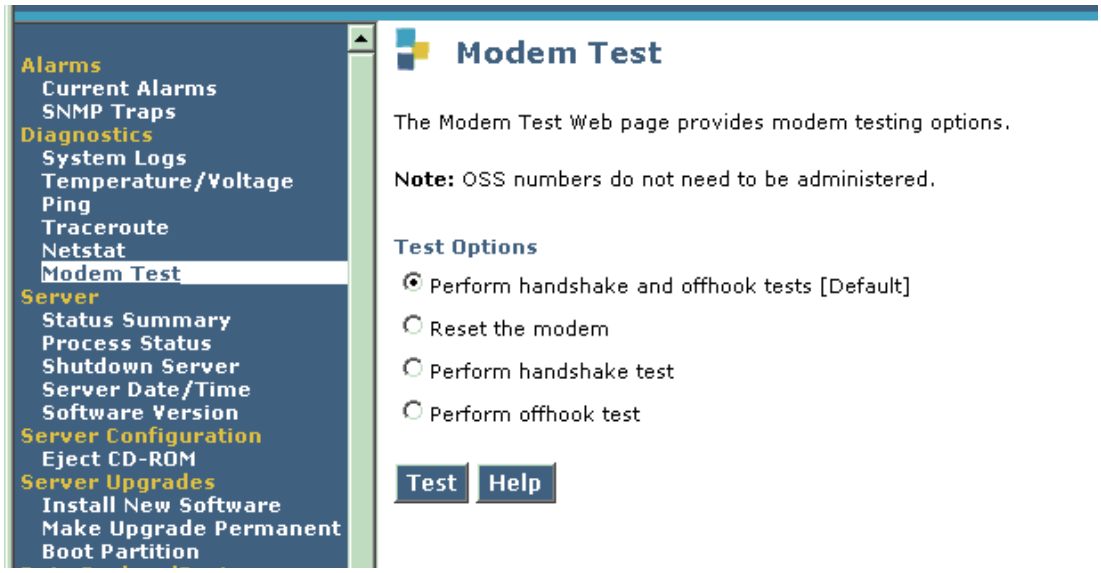
I-Node is the associated file for this socket, shown as an I-node number.

Path is the path name of the processes attached to the socket.

Modem Test screen

Use this screen to test the modem and ensure it is working properly. The modem reports Avaya server alarms (see Alarm-reporting options for details). It also enables you to dial in to an interface through which you can fix problems as they occur.

Figure 106: Modem Test screen



Modem Test screen field descriptions

Test Options

Use these steps to test the modem:

1. Select one of the following tests by clicking the corresponding radio button:
   - **Performs handshake and offhook tests**. Choose this default selection to run both the handshake and the offhook tests. If these tests fail, run the handshake test and the offhook test individually to determine the reason for the failure.
   - **Resets the modem**. Choose this selection to reset the modem.
   - **Performs handshake test**. Choose this selection to verify that the modem is connected to the USB port and responding (that is, the drivers are functioning and the modem is sane).
   - **Performs offhook test**. Choose this selection to take the modem offhook and search for a dial tone. This test is important because some configurations have two modems, one for each server, and the modems share a single analog line.
2. Click **Test**.

Troubleshooting modem problems

To verify that your modem is functioning properly, use the following procedure to test for problems.

If the handshake test is successful, run the offhook test.

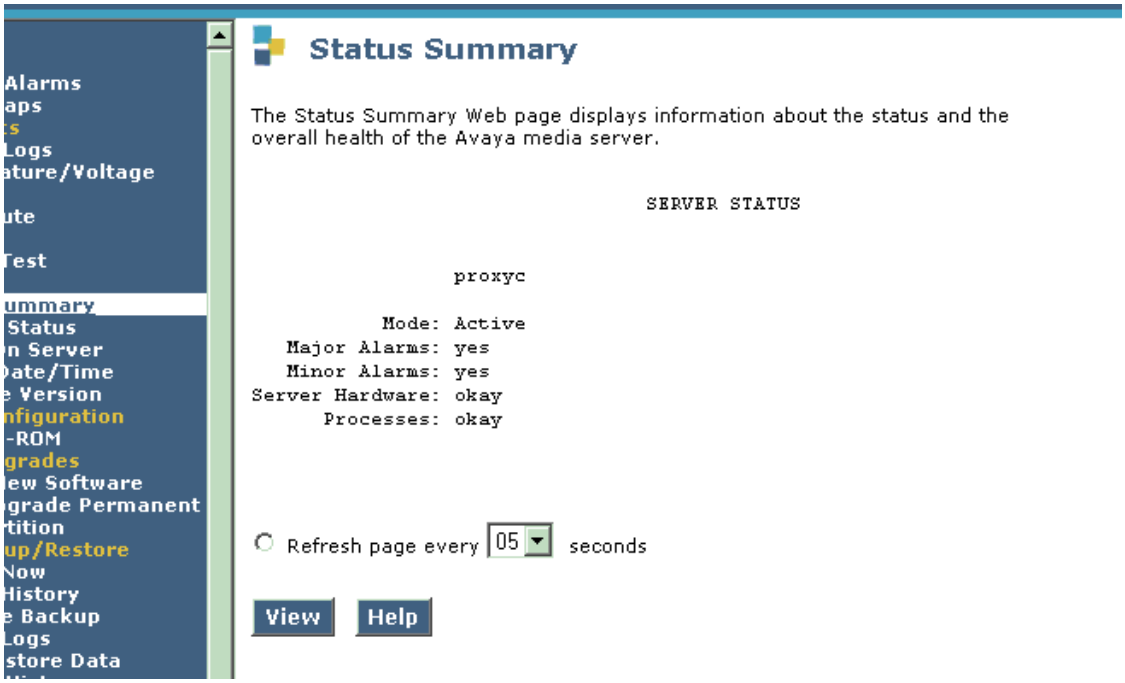
1. Run the handshake test. If the handshake test fails, check the modem connection to the telephone line and the server, make sure the modem is powered on, and then continue with Step 2.
2. Run the handshake test again.
3. If the handshake test is successful, run the offhook test. If the offhook test fails, check the modem connection line and hardware, then continue with Step 4.
4. Perform the offhook test again.
5. If either the handshake or the offhook test fails again, reset the modem.
6. After you reset the modem, run the handshake and offhook tests again. If you get an output message stating that the tests were unsuccessful because they failed to open a device (tty), it indicates that some other program is using the modem.

   In this case, check to see if someone else is using the modem.
7. If there are no problems with the connection line and hardware, restart the server.

Server screens

Status Summary screen

Figure 107: Status Summary screen



Status Summary screen field descriptions

Use the Summary Status page to quickly see virtually everything you need to know about Avaya server status. For example, you can view duplication status information about both servers from this page, and see which server is in primary or backup mode. In addition, you can see the following state-of-health/status information about your server or servers.

Mode

(Read-Only) This shows whether the server is primary or backup.

Major Alarms

(Read-Only) This shows whether this server has any Major Alarms, **yes** or **no**.

Minor Alarms

(Read-Only) This shows whether this server has any Major Alarms, **yes** or **no**.

Server Hardware

(Read-Only) This shows whether the server is **okay** or otherwise.

Processes

(Read-Only) This shows whether the processes running on the server are **okay** or otherwise.

Server Status

To view overall status information about the servers:

- Information about server duplication appears on the top part of the page.
- Information about the server's mode and state of health appears on the bottom part of the page.
- For detailed information about the fields on the Status Summary page, see Status Summary screen field descriptions on page 363.
- To refresh the page periodically: Click **Refresh page every __ seconds**. Select the number of seconds to wait before a page refresh (or accept the default value).
- Click **View**.

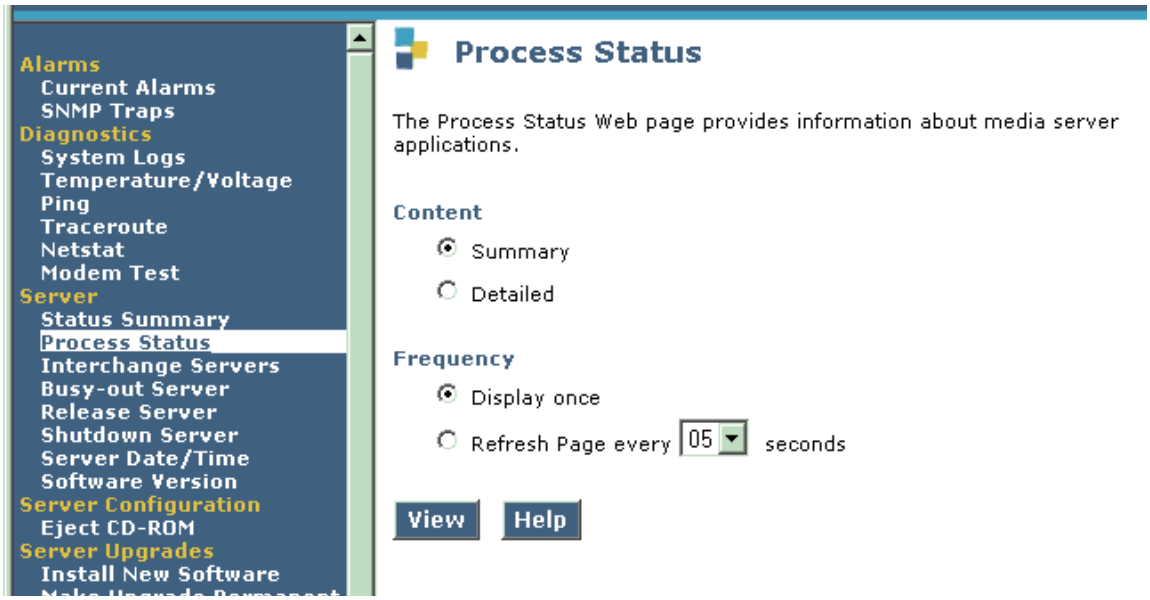
Note:

You *must* select a value in the **Refresh page repeatedly every 05 seconds** drop down list before you click View, or the system displays an error message.

Process Status screen

Use the Process Status page to view status information of server applications. Each application is a collection of processes. View information about each entire application or its individual processed. You can also choose whether you want a static display or one refreshed periodically.

Figure 108: Process Status screen



Process Status screen field descriptions

Content

Summary. This default option provides information about each server application as a whole, including a count of the application processes running compared to the total number of processes available (for example, 2/16). It also shows if the application is up, partially up, or down.

Detailed. This option provides the same information as the summary display, but also provides information about each of the processes associated with each server application.

Frequency

Display once. This default option displays the status results once in the Process Status results page. The page is not refreshed even when the status changes.

Refresh page every 05 seconds. This option displays the status results every few seconds, based on the value you select from the drop-down box.

Note:

These settings apply to both the summary and detailed displays.

Click **View** to display the process status for all the server applications.

Troubleshooting partially up processes

This procedure is for home servers only.

PARTIAL UP is an indication of the initial state of the sipserver and eventserver processes when these cannot get the needed SES server setup information from the database.

When watching this screen for the correct progression of processes, the Partially Up status may not transition for these three processes:

- sipserver
- eventserver
- imlogger

There are several possible root causes:

- Postgresql service is not up
- Postgresql service is up, but the database schema was not set up properly
- The database schema has been set up, but does not have the initial setup information of the SES server, such as domain information, media server information, licenses, passwords, and so on.

In the list above, the first and second items are unlikely if the installer had success with the ccsInstaller script.

The third item, no or incorrect setup information, is the most common cause. Forcing a duplexed server interchange does not resolve the problem. Instead, take one of the following actions:

- Provide the setup information through administration screens. Check all the fields on these screens for correct information:
  - Domain screen
  - Media Server screen
  - Host screen
  - Configure Server screen
  - Authentication File screen

- Restore the database from previous backup.
- Perform **Force All** on the edge server.

  This pushes the database information onto this home server.

Process Status results

This page displays status information for the server applications based on the selection you made on the Process Status screen on page 365: Summary or Detailed. Regardless of which view you chose, status information appears for the following applications:

Application Name	Description
Watchdog	Brings the system up, recovers from failures, and brings the system down cleanly.
TraceLogger	Creates and maintains the log files where most applications running on an Avaya SES server write messages.
INADSAlarmAgent	Sends alarms to the Initialization and Administration System (INADS) using SNMP traps defined in the INADS MIB.
CCSTrapAgent	Acts to send Simple Network Management Protocol (SNMP) traps defined for SES.
GMM (Global Maintenance Manager)	Collects, processes, and reports system-wide alarms.
SNMPManager	Acts as the SNMP trap receiver for the server. The received traps are decoded and written to the syslog.
ImLogger	Creates and maintains the log files where the Instant Messaging application writes messages.
SipServer	Controls the SIP communications sessions and their associated messaging. (Is not running when in backup mode.)
drbdEventSvc	The distributed redundant block device synchronizes database information between duplex servers.
MtceMgr	The Maintenance Manager monitors application alarms and mon information to determine when to interchange servers for local failover in a duplex server configuration.
mon	Monitors system health via certain processes on the primary server. When these required processes fail to respond to mon, this signals an interchange of servers may need to occur.
SME (Server Maintenance Engine)	Tests server components periodically. The SME tests components as the result of both specific requests and asynchronous errors.

Shutdown Server screen

The Shutdown server page indicates whether the server is a primary or backup server. Also use this server page to safely bring down the server immediately or later on, and whether it reboots after the shutdown.

Figure 109: Shutdown Server screen

Realize that when you Shut down this server, the web server stops the process in which you are communicating. You can not access the web pages until the system starts.

Shutdown Server screen field descriptions

Options to Shut down

Delayed Shutdown. When you choose this option (the default), the system notifies all processes that the server will be shut down. The system waits for the processes to close files and perform other clean-up activities before it shuts the server down.

Immediate Shutdown. When you choose this option, the system does not wait for processes that are running to terminate before it shuts the server down. Data may be lost.

Restart Server after shutdown. Select this option to reboot after shutting down.

Shutdown even if this is the primary server. Select this option if this server is the primary one.

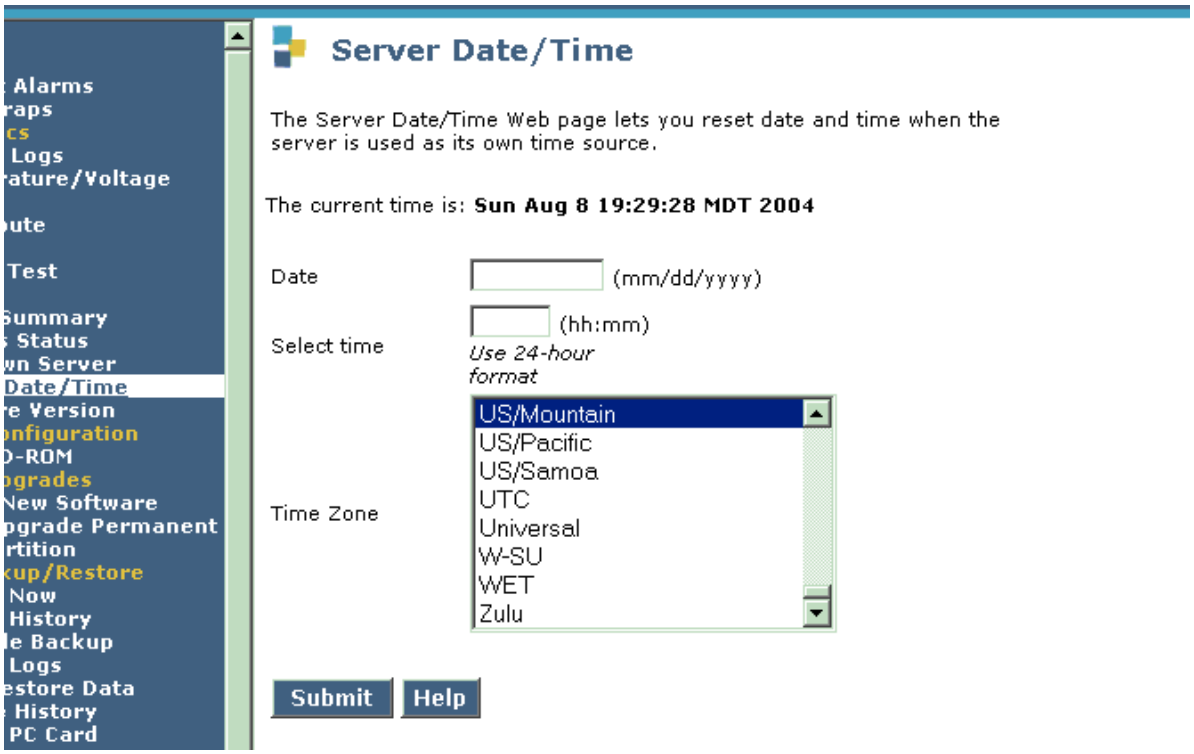
Click **Shutdown** to begin the process.

Server Date/Time screen

Use this page to set or adjust the time on a new or in-service Avaya server.

Compare the use of this screen with Network Time Server screen fields on page 376.

Figure 110: Server Data/Time screen



Server Date/Time screen field descriptions

The Avaya server can use its own clock as a time source, or be synchronized with an external time source on the corporate network.

- If this server is using its own clock as a time source, use this page to adjust the time. General Notes on Timeserving on page 370.
- To use Network Time Protocol (NTP) see Configure Server on page 372.
- If the Avaya server is synchronizing its time with a Network Time Server (NTS) external time source, set the time using this page *only* during initial configuration to bring the server's time close enough to the NTS's time so that synchronization can occur (within about 5 minutes).

CAUTION:

If synchronization with an external time source is enabled, do not use this page to adjust the time after the server is in operation. Time changes greater than 15 minutes will disrupt the synchronization with the NTS and NTP will shut down.

General Notes on Timeserving

The Avaya SES software relies on the time of day setting for many system functions, including these:

- Time stamp data elements (including error logs and record files)
- Set time-out intervals (including automatic wake-up messages and do-not-disturb intervals)
- Perform scheduled tasks (such as system maintenance and backups)
- Synchronize time of day with other processors on the network.

Out-of-sync timing messages are ignored, so an outsider cannot easily reset the server's clock by sending it a wildly inaccurate time.

CAUTION:

The page displays the current time near the top of the page. If an Avaya server is synchronizing its time with a Network Time Server (NTS) external time source, you only set the time during initial configuration to bring the server's time close enough to the NTS's time so that synchronization can occur (within about 5 minutes). Do not use this page to adjust the time after the server is in operation. Time changes greater than 15 minutes disrupt the synchronization with the NTS.

Date

Enter the month, day, and year.

Double-check your day entry.

If incorrect, the server will adjust it. For example, if you enter February 31, the server changes it to March 3 on the results page. If you do not select a year, it supplies a default year, which may not be current.

Select Time

Enter the hours and minutes.

Time Zone

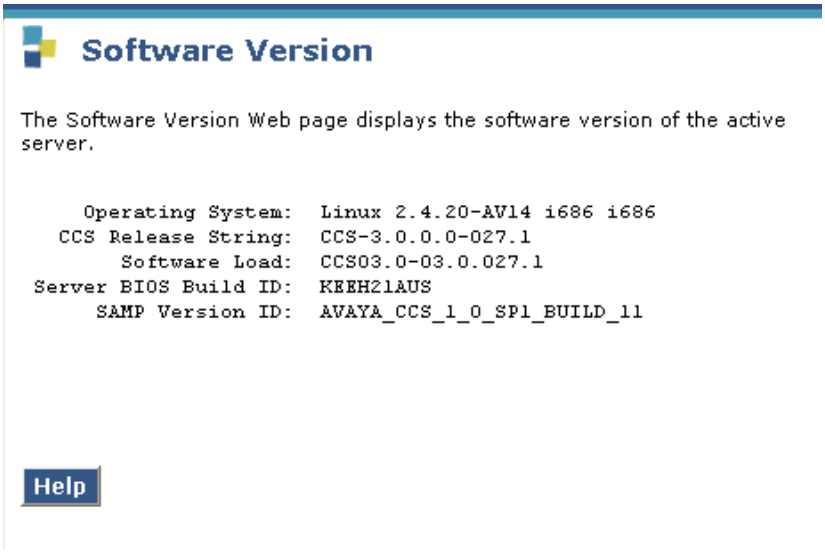
Using the scroll box, choose the correct time zone for this server's location. If you reset the time zone, the call-processing software needs to be restarted.

Click **Submit** when you are satisfied with the settings.

Software Version screen

Use the Software Version page to determine the software version, BIOS, and firmware this Avaya server is running. You may want to check your software version before, during, or after you install new software. This screen is also helpful during troubleshooting.

Figure 111: Software Version screen



Software Version screen field descriptions

Operating System

(Read-Only) The release and issue number of the Linux operating system that is running on the server. For example:

Linux 2.4.20-AV14 is the release (by field: major release, minor release, development release - subrelease, Avaya release). **i686** is the processor type.

CCS Release String

The release and issue number of the Avaya software that is running on the SES server. For example:

CCS-3.0.0.0-027.1 is the release (by field: major release, minor release, development release, Avaya build).

Software Load

CCS03.0-03.0.027.1 is the full version of the software release name. The major release, minor release, development release, subrelease, followed by the load number, such as 037, that increments for each new software build, and the final number, an additional release number, for internal use only.

Server BIOS Build ID

This label shows the build ID of the BIOS of the server. This information is critical at install time, but can be checked at any time, perhaps as an aid in troubleshooting.

SAMP/RSA Version ID

This field shows the firmware version of the SAMP or RSA remote maintenance board. This ID must be correct at install time, but you may check it at any time. If you find that your SAMP/RSA version is incorrect, use the procedure Verify firmware on the SAMP module on page 93.

Server Configuration

Server Configuration items consist of these two choices:

- Configure Server on page 372
- Eject CD-ROM screen on page 383

Configure Server

The Configure Server item under the Server Configuration section of the menu contains four screens:

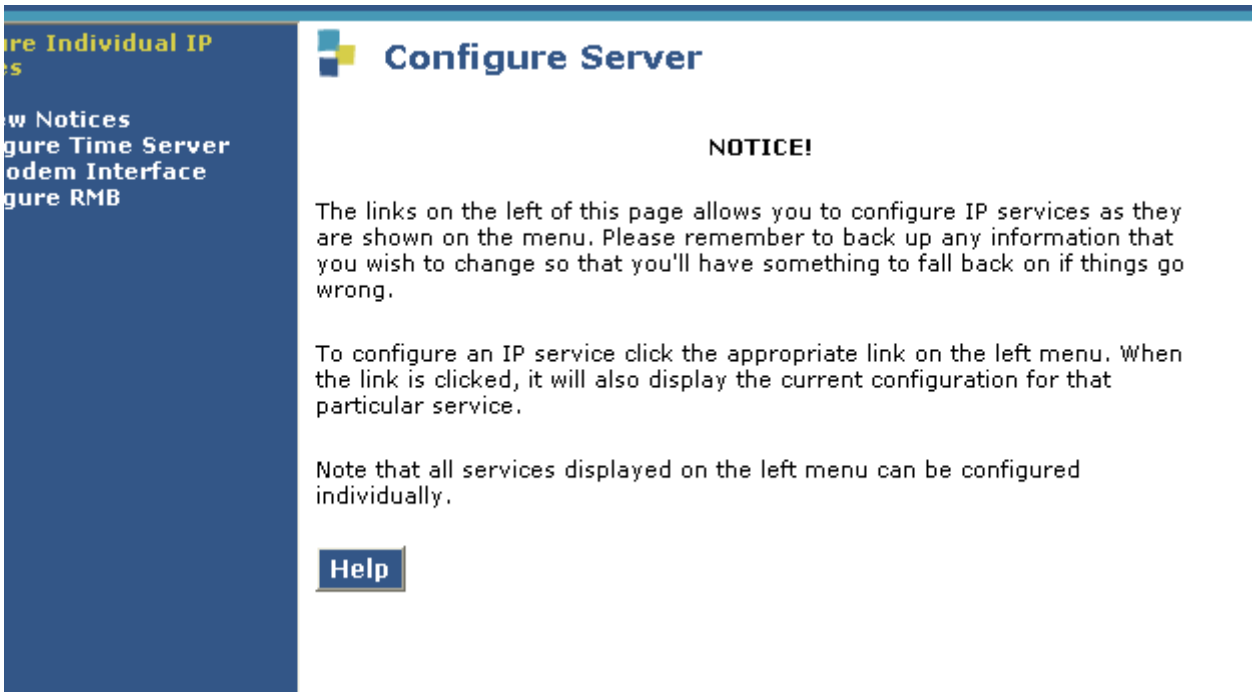
- Notices screen on page 373
- Network Time Server screen on page 374
- Network Time Server screen fields on page 376
- Set Modem Interface screen on page 378

These screens provide a web interface to perform the tasks implied in their name.

Notices screen

Figure 112 provides an overview of this section of screens.

Figure 112: Configure Server—Notices screen



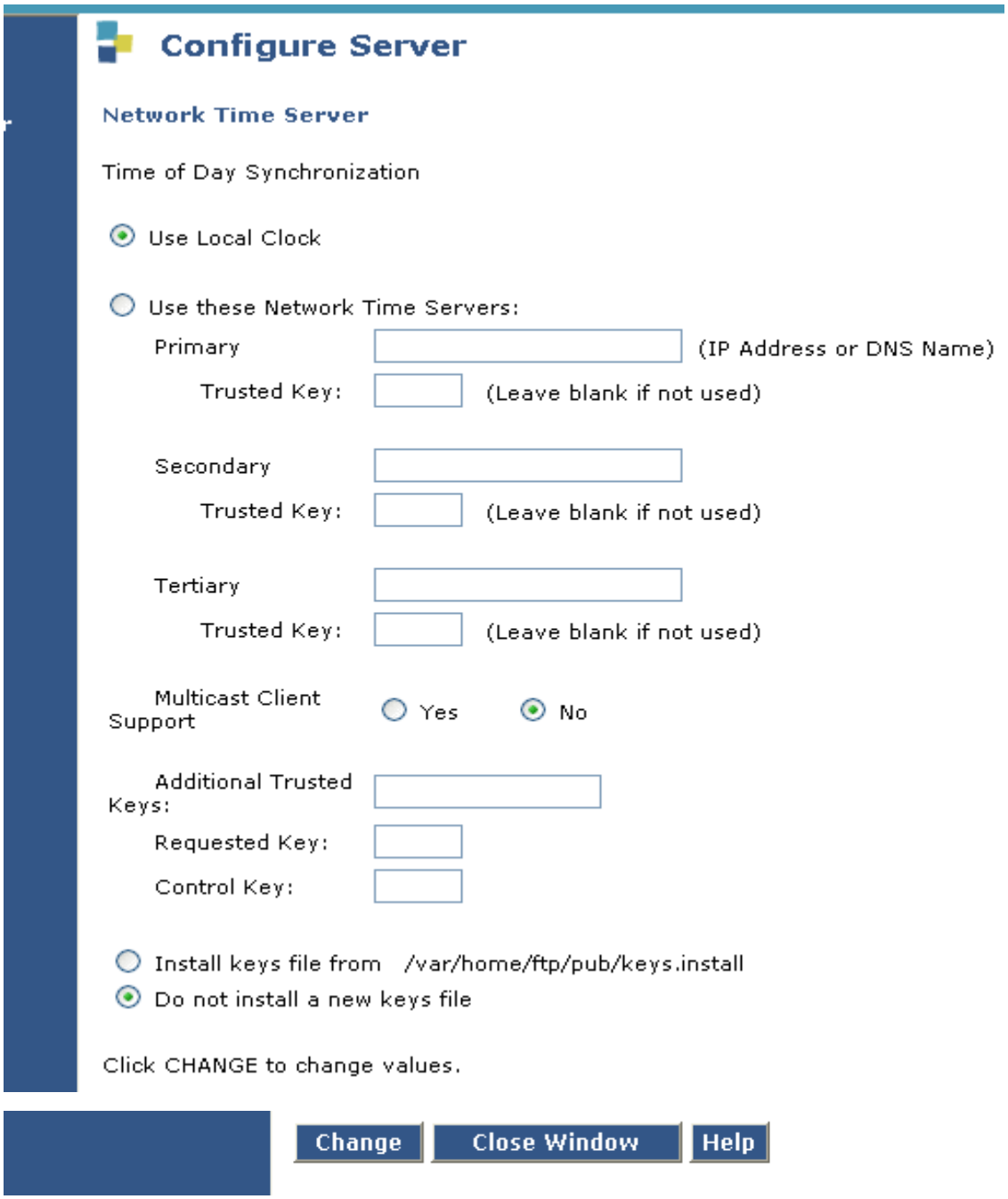
Network Time Server screen

Use the Configure Time Server page to specify the time source that the SES server uses to set the time of day. The time of day of the server can be controlled by its local clock or it can be controlled by an external time source on the corporate network.

To set the date and time on the server's local clock, use the Server Date/Time page.

Also see Server Date/Time screen on page 369 to compare and contrast.

Figure 113: Configure Server—Network Time Server screen



Network Time Server screen fields

Time of Day Synchronization

To specify the time source for the Avaya server, choose either **Use Local Clock** or **Use These Network Time Servers**.

Use Local Clock

If this server is to use its own clock, choose the Use Local Clock button and adjust the time on the Server Date/Time page.

Use these Network Time Servers

- If this server is to synchronize its clock with a Network Time Server, choose the **Use these Network Time Servers** button. At initial installation, adjust this server's time on the Server Date/Time page. The setting should be within 5 minutes, if possible, of the NTS's time for synchronization.
- Specify up to three network time servers by IP address or DNS name in the order you want the SES server to check them. Primary, Secondary, and Tertiary is the sequence in which the SES server will check the time servers. Enter IP addresses or DNS names for the primary, secondary, and tertiary servers. Leave extra fields blank if you use only one or two servers.
- **Multicast Client Support**
  - Select **Yes** if the NTS routinely broadcasts its timing messages to multiple clients.
  - Select **No** if the Avaya server is to poll on request the time directly from the NTS.
- **Additional Trusted keys**: Functions like a checksum to make sure the time packets are valid.
- **Request key**: Allows an administrator to send a remote query request.
- **Control key:** Allows an administrator to query and request changes to an NTS.

Providing The Keys.install File

If encryption between the NTS and Avaya server is to be used for additional security, you must provide a keys.install file that specifies for each key: Key number, Encryption type, and Key code.

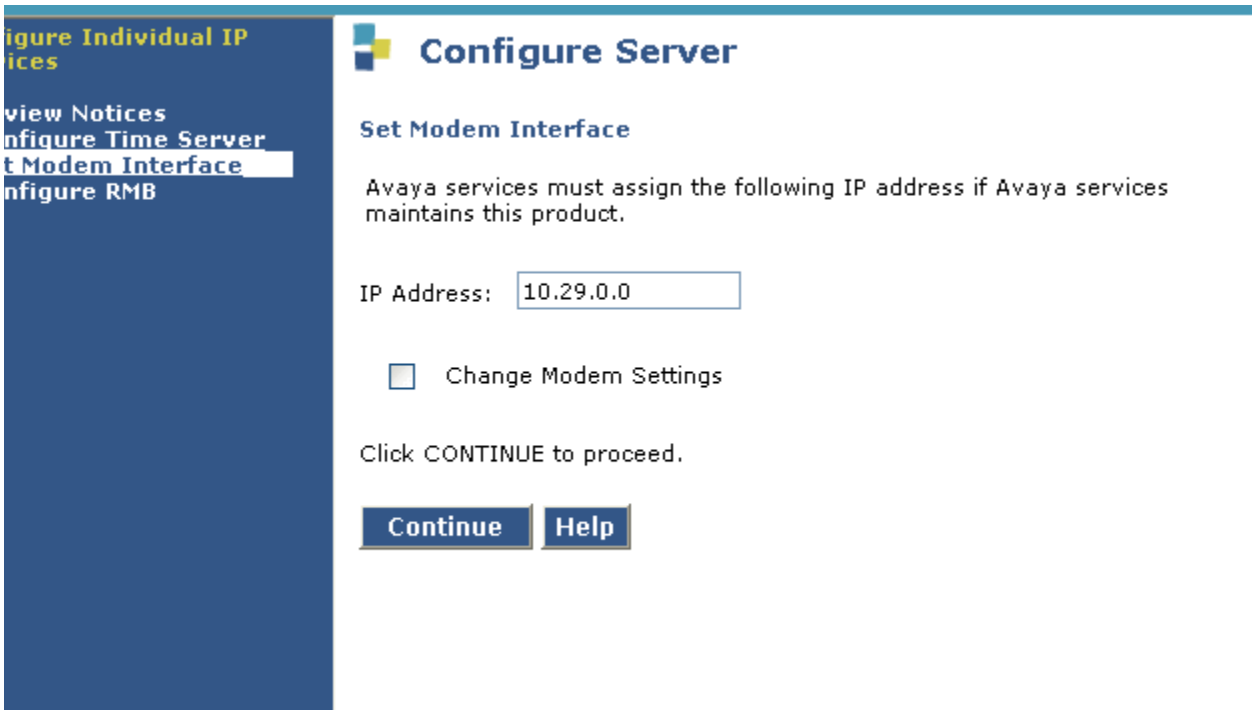
- **Install keys file from /var/home/ftp/pub/keys.install:** Locate the keys.install file on your computer or network, then click Load File. The file is uploaded to the /var/home/ftp subdirectory.
- **Do not install a new keys file:** Lengthy key files can be transferred from the network time server to the Avaya server as follows:
  - Use the Download Files Web page. The file is transferred to the /var/home/ftp subdirectory.

Select **CHANGE** to confirm the changes in the values.

Set Modem Interface screen

Use the Set Modem Interface screen to enable Avaya services, or another trouble-tracking service, to monitor your SES server for alarms. Also, Services personnel can dial into this interface to fix problems as they occur. If an Avaya maintenance contract is in place, the values on this page must be provided by the Avaya services center.

Figure 114: Configure Server—Set Modem Interface screen



Set Modem Interface screen field descriptions

IP Address

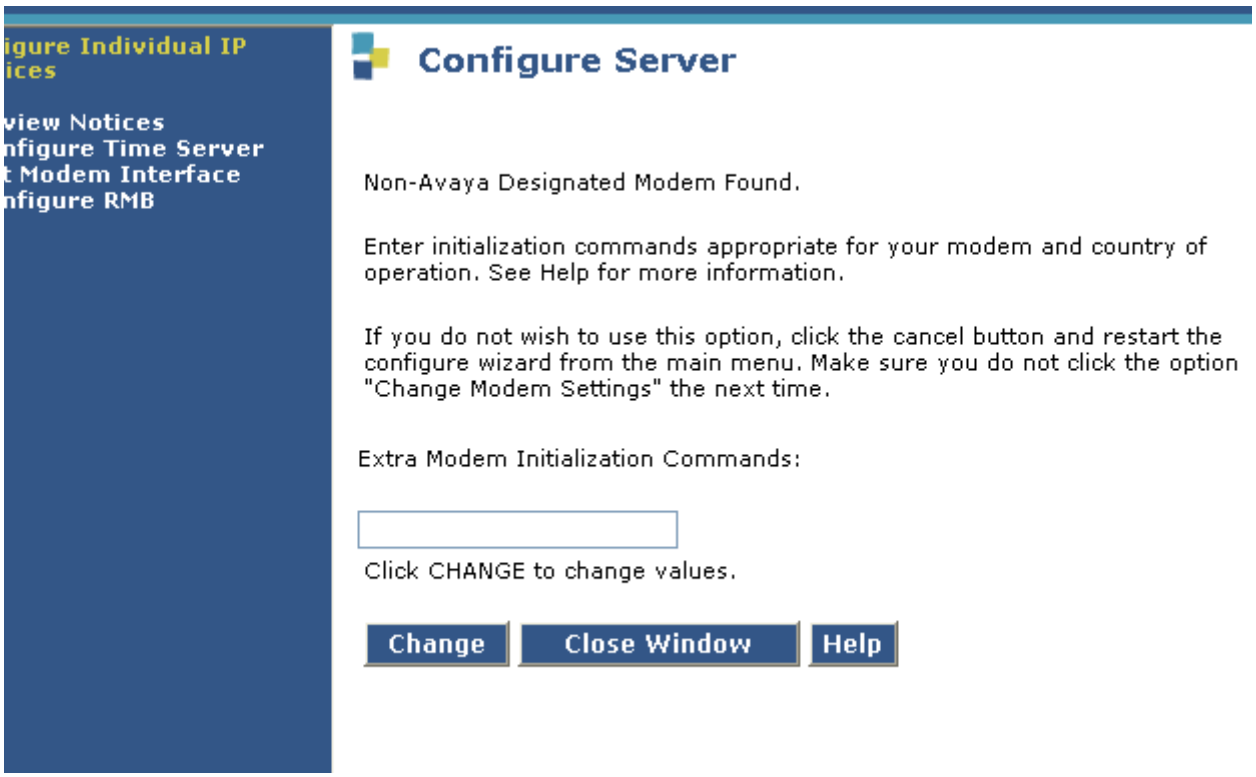
If this system is serviced by Avaya Services, a modem IP address should already be entered in this field. If the system is not serviced by Avaya, consult with your maintenance provider for the correct IP address.

Change Modem Settings

Select the check box ONLY to change to modem settings different from the factory defaults. You most likely do not need to change settings of an Avaya-recommended modem (MultiTech MT5634ZBA-USB-V92) manufactured in the United States. However, if the modem is purchased in another country, possibly its default settings are US-configured and subsequently must be changed according to the country.

If you need to change modem settings, select the check box and click **Continue**. You will be taken to a page beginning with the message **Non-Avaya Designated Modem Found**.

Figure 115: Non-Avaya Modem screen



If you are using a MultiTech MT5634ZBA-USB-V92 modem installed in the United States, most likely you DO NOT need to change the initialization settings. If, however, you are using a different modem, or you will be using the modem outside the United States, you may need to change these settings.

If you decide at this time that you do not need to change modem settings, click **Close Window** and re-launch the Maintenance Web Interface.

To proceed with changes, you must make entries in the form of AT commands in the **Extra Modem Initialization Commands** field. Multiple commands can be entered, each separated by a semicolon. If your modem is a MultiTech MT5634ZBA-USB-V92, you can link to the Country Commands table for the modem settings appropriate to your country. If you do not have a MultiTech MT5634ZBA-USB-V92 modem, see your modem documentation.

For example, to change the country code from US to Japan, enter on this web page: AT%T19,0,10

Note:

The command for the United States is AT%T19,0,34, the same modem code used by many countries.

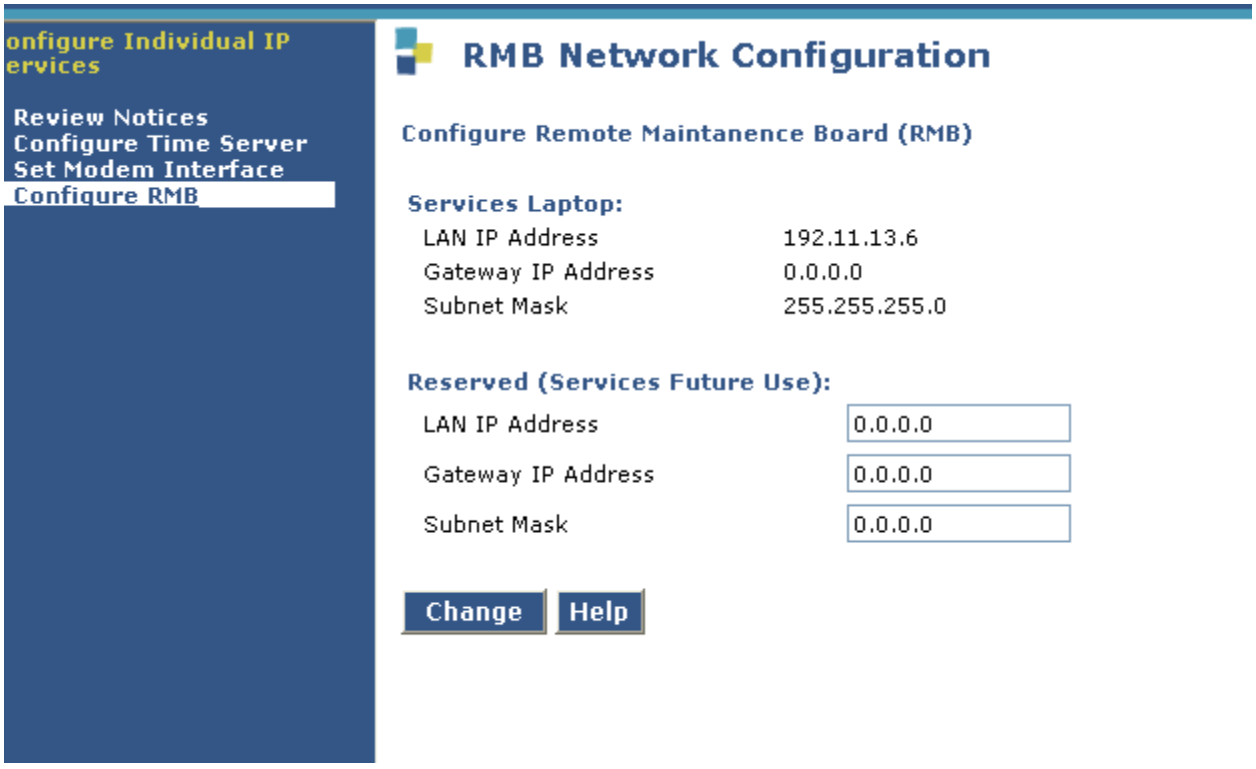
RMB Network Configuration screen

Use this page to configure IP connectivity for the Remote Maintenance Board, either RSA or SAMP, installed in the SES server.

The RMBs installed in the S8500 and S8500B servers are different. The Remote Supervisor Adaptor (RSA) is installed in the S8500, and the Server Availability Management Processor (SAMP) board is installed in the S8500B.

Either RMB allows remote management of the SES server. This board simplifies system management by providing around-the-clock remote access independent of server status.

Figure 116: Configure Server—RMB Network Configuration screen



RMB Configure screen field descriptions

Services Laptop

These settings (LAN IP Address, Gateway IP Address, and Subnet Mask) for the local Services port on the RMB are configured automatically during server installation. They are displayed as read-only on this page for the S8500 server.

Reserved (Services Future Use) (Optional)

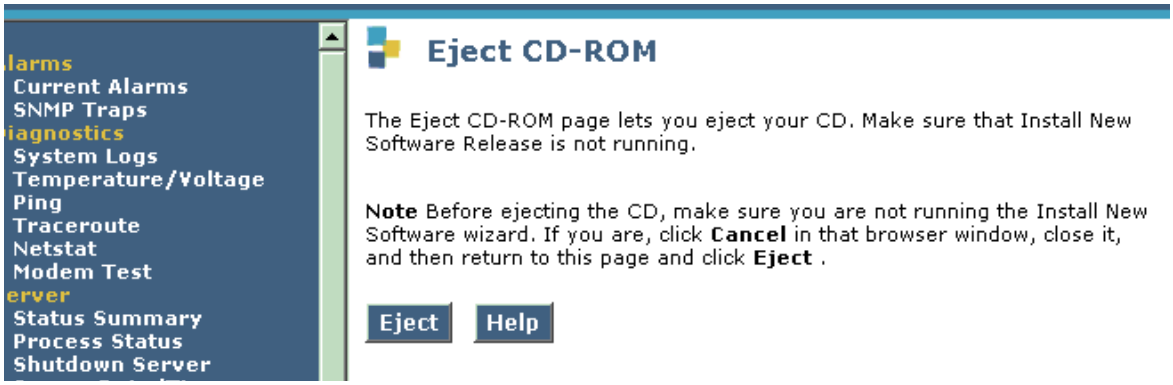
This section is applicable to only S8500B servers.

The LAN IP Address, Gateway IP Address, and Subnet Mask for the eth1 interface on the SAMP board are configured on this page. This interface can provide access to the SAMP from the customer's network. The customer's network administrator must provide the values for these settings.

To modify these settings, enter new values in the three fields and select **Change**.

Eject CD-ROM screen

Figure 117: Eject CD-ROM screen



Eject CD-ROM screen field descriptions

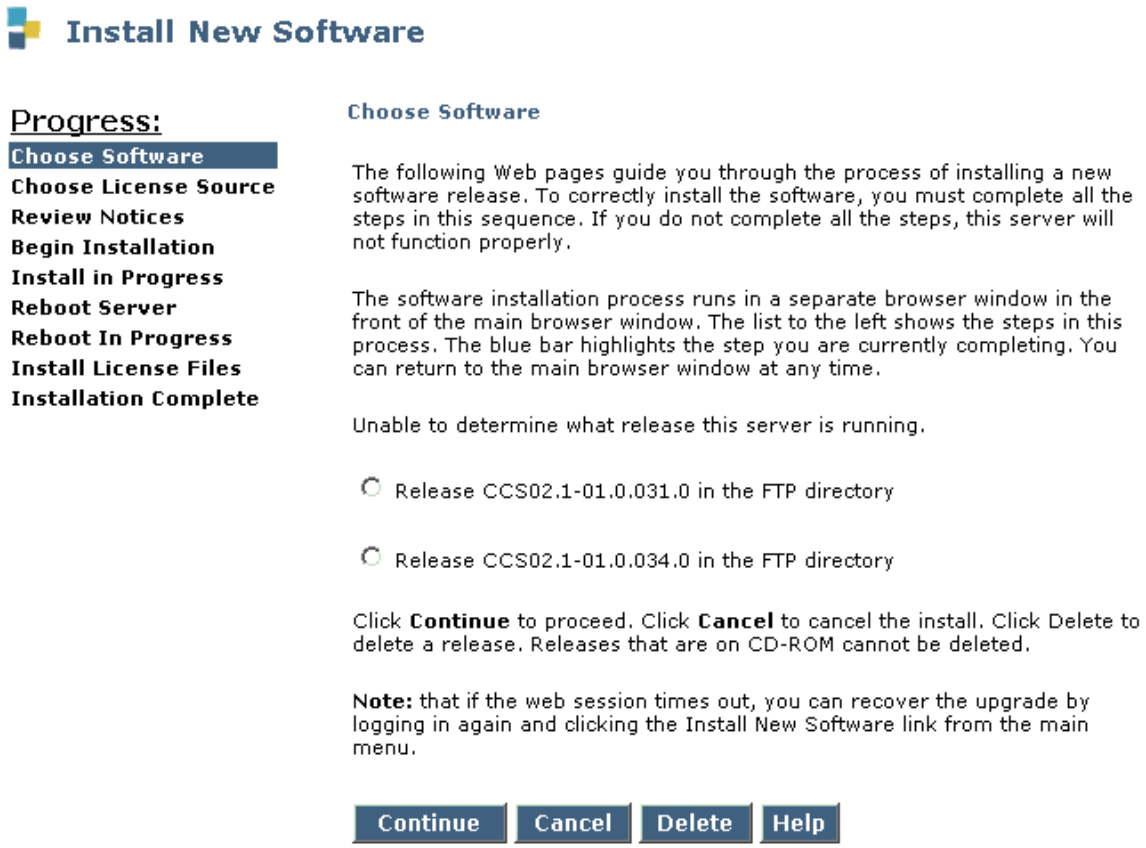
Eject

Use the Eject CD ROM page to eject the software application CD. Before you eject the CD, make sure you are not running an Install New Software Release procedure. If so, click Cancel from that browser and close it. Return to the Eject CD ROM page, and click the **Eject**.

Server Upgrades screens

Install New Software screen

Figure 118: Install New Software screen



Install New Software Wizard Steps/Pages

Choose Software

The Choose Software page is the first page of the Install New Software wizard. Run this wizard to upgrade software on the server.

- Install new software from a laptop computer in the server room, an administration computer over the network, or a remote computer using a PPP dial-up connection.
- Install new license or authentication files to install new software.

To select software for installation, click one of the radio buttons to find the software files. For example,

- Release CCS R3.0.0.0 in the FTP directory on the server's hard drive.

  Note:

  The `software_releases` subdirectory on the server's hard drive, contains the current software load that the server is running, and is used only to reinstall the current software.

- Release CCS R3.0-01.0.0.0 in the CD-ROM drive of the server

Click ***Continue*** to finish the installation, or **Cancel** to stop the process.

Note:

If the system cannot locate software installation files, an error message appears. To resolve this:

- If you have a CD-ROM containing new software, make sure it is installed in the drive of the Avaya server that you are currently logged into.
- If Avaya remote services copied new software to the server, a copy should exist in the FTP directory on both servers.

Choose License Source

You must have a software license file before you install this software release. If you do not have this file available, use tools in the main window to transfer it to the system. DO NOT continue this installation until it is available.

In the screen representation below, always choose the second option AND the third option.

Select a source for the license files:

- I will supply the license files myself when prompted later in this process.
- **I want to reuse the license files from the currently active partition on this server.**

  It is not normally necessary to update the authentication information, but if the new software documentation instructs you to, you may update it as well.
- **Do not update authentication information.**
- Update authentication information as well as license information.

Click **Continue** to proceed. Click **Cancel** to cancel the install.

Review Notices

What you need to know about the Install Software Wizard:

Install New Software wizard: Use this to upgrade the software running on the server. Access this wizard from the Maintenance interface item **Server Upgrades**.

Moving backward or forward in a wizard

The wizards are used serially. If you change any data:

- Install New Software wizard: Cancel the installation wizard, and run it again. This is the safest way to prevent possible problems.
- The first time you run this wizard, a lot of data are entered manually. If you need to change something you entered on a previous page:
  - Use your browser's Back button to page back through the Configure Server screens.
  - Check or change the item.
  - Always click **Continue** to move forward, whether you change anything or not. If you do not do this, information in the wizard may not be processed correctly.

You can (if desired) cancel the Software Wizard, and run it again from the beginning.

Running the wizard after a session time-out

All Web pages time out if left inactive for 30 minutes (see Log Off). If this occurs while you are using one of the wizards:

1. You see a session time-out message in the main web administration interface window.
2. You must log in again, then:

Install New Software wizard: You have the option to resume the installation. When you click the Install New Software Release link, you see a message saying that a session is already in progress. If you choose to take over the session, the wizard will return you to whatever point the installation was interrupted.

CAUTION:

If you lose data after a time-out, you must re-enter the data manually. Run the configuration procedure in one session without interruptions greater than 30 minutes.

Using progress indicators

Each wizard lists the steps (screens) in the wizard along the left side of the window. The page that you are working on currently is highlighted. This listing is provided to show your progression through the wizard. The screens cannot be used for navigation (to back up or move forward in the wizard).

Working with the wizard window

When you click the Install New Software in the main web administration window, the wizard pops up in a new window on your page. You can switch between this window and other windows on your computer using the features supported by your computer, such as Alt+tab or your computer's task bar.

Begin Installation

Use the Begin Installation page to verify your software installation options before you begin the installation.

To start the installation:

1. Review the software and license file information on the page to make sure it is correct.
   - If you need to make any changes, click Cancel and run the Install New Software wizard again.
   - Once you verify the information is correct, go to 2.
2. Click **Continue** to proceed. At this point, the server:
   - Copies the currently active software to the inactive partition.
   - Unpacks the new software files and copies them to the inactive partition, and prepares the server to reboot from the new software. This preserves any translations and modifications made to the active software. This takes several minutes, and the status appears on the Install in Progress page.

Install in Progress

This Install in Progress page displays the status of the server copying and unpacking software files, and preparing to reboot from the new software release. The Reboot Server page automatically appears when this process is complete. During the installation-preparation phase, choose either of the following options, if available. The button options on the page change as the installation progresses:

1. **Refresh**. Update the progress display instantly.
   - If you click **Refresh**, the status of the software installation is instantly updated and reported to the page.
   - If you do not click **Refresh**, the status of the software installation is updated and reported to the page every few seconds.
2. **Cancel**. This button only appears if the software installation fails. If you see this button:
   - Review the progress information for clues about why the installation failed.
   - Click the **Cancel** button to close the Install New Software window.

   CAUTION:
   If the software installation fails or you cancel it, the partially installed software release remains on the server's hard disk. You will see this entry the next time you access the Choose Software page.
   - If the software did not install correctly, you must install it from the original media.
   - If you cancelled the installation, install this software again.

Reboot Server

At this point in the software installation, all new software files have been copied to the inactive partition on the server's hard drive. When you reboot the server, the partition containing the new software will come up as the new active partition. This is the final page that appears before the new software is installed.

CAUTION:
When you reboot the server to install the new software, service may be interrupted.

Reboot Procedure

Before you reboot the server:

1. Check the message at the top of the page to verify that the software was copied successfully.
   - If the copy was successful, go to Step 2.
   - If the page indicates any problems, see Problems during software installation.

2. Understand the impact that this software installation may have on current telephony service, summarized in Service impacts below.
   - If you are working on the primary server and a backup server is available, Interchange Servers now to minimize any impact on call processing.
   - If the server you are upgrading is not yet in service, it will give you a primary server warning. Proceed in spite of this warning.
3. Make sure you are ready to reboot the server.
   - This is your last chance to Cancel the software installation. If you want to make any changes, click **Cancel** now, then run the Install New Software wizard again.
   - If you are ready, click **Continue**.

While the server is rebooting, you will not be able to access any web administration interface screens.

Service Impacts

When you click Continue to install new software:

- If you have only one Avaya server (no operational backup server is installed) all calls will be dropped, and service will be unavailable for up to 15 minutes while the server reboots.
- If you are working on the primary server and a backup server is available, service will continue as follows:
  - The servers will automatically interchange. Some transient (non-stable) calls in progress may be dropped when this happens.
  - Service is now available on the new primary server. The server that you are logged into becomes the current backup server.
  - The current backup server is now busied out, then rebooted to install the new software.
  - If you are working on the backup server, call processing is unaffected during the 15 minutes that the server needs to reboot. If for some reason the primary server attempts to interchange during this period, it will be unable to do so, and service may stop until the reboot completes and this server is made primary.

Reboot in Progress

When you reboot the server, it can no longer communicate with the web administration interface. The Reboot in Progress web page remains on your page until the reboot completes.

While the server reboots:

1. The Reboot in Progress page displays an initial reboot message, then pauses until the reboot is complete and the server is ready to proceed.
   - Allow up to 15 minutes for the reboot to complete.
   - Although the Continue button is visible, do not click it yet. See step 3.
2. Optional. To check status during a reboot, you may try the following:
3. Ping the server by name or IP address using a ping program on your computer. Use the option to run the ping continuously. When ping can find the server, basic data communication through the physical connection is in place. The other services will be starting up shortly.
4. Open a telnet session on your computer and try to access the server by name or IP address. When telnet responds, the software has started up and the web pages will be available soon.
5. When the reboot should be complete, click the **Continue** button.
   - If the reboot is complete, the Install License Files page appears.
   - Run some basic software verification tests before proceeding.
   - When basic tests are complete, return to the Install New Software wizard window and continue with the software installation.
   - If you click Continue and nothing happens, the reboot may not yet be complete. Wait a couple of minutes for the Install License Files page to appear.

Occasionally your Continue request may time out and you'll see a Can't Access The Server warning. If this happens, either:

- Reload or refresh the web page to submit the Continue request again, or
- Click the browser's back button to return to the Reboot in Progress page, then click **Continue** again.

When the Install License Files page appears, proceed.

CAUTION:

If the reboot is unsuccessful, the following may happen:

- An error message may appear and the server comes up running the previous version of software.
- The server may simply cease to respond.

Install License Files

This Install License Files page display varies on the option you chose from the Choose License Source page:

- ***Supply files when prompted***. You must upload the correct software license and Avaya authentication files to the server using screens in the main web-administration interface window.
- ***Copy files from duplicated server***. If the duplicated server already has the correct copy of the software license and Avaya authentication files, the files are automatically copied from there to the correct directory on this server. If this copy procedure fails, see Problems during software installation.
- ***Reuse files on the primary partition of this server***. No new license and authentication files are needed. This page does not appear.

Click **Continue** to proceed to install the license files.

Installation Complete

The software is now installed. It must be verified for correct operation, then made permanent.

To complete the software installation process:

1. Review the information on the page to verify that the new software was successfully installed.
2. Click **Close** to exit the Install New Software wizard window.
3. Verify software operation and make the server upgrade permanent.

Make Upgrade Permanent screen

This **Make Server Upgrade Permanent** screen is the last step required for completing the installation of a new software release. It sets up the server to reboot from the currently primary (new) software version, instead of rebooting to the previous version.

- You do not need to change the server status to backup.
- Because the Install New Software wizard must be run on each server to upgrade it, you need to use this page on each server after you complete a software installation.

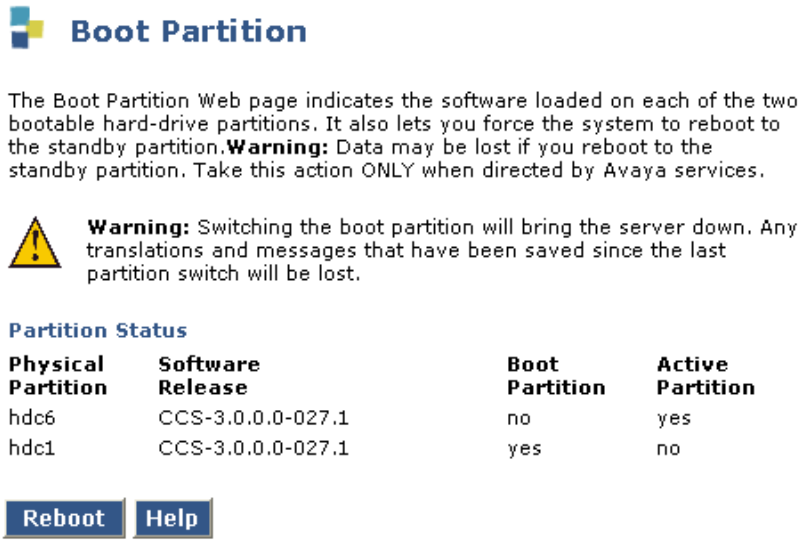
If you do not commit the new software release (make it permanent), then the next time the server reboots, it runs the previous software version. Any new translations you made to the new release will be lost, and the new software must be installed again. You should commit the new software to operation when you are satisfied that it is functioning.

1. To make a new software release the new permanent version, click **Submit**.
2. Check that the request to commit the new software (make it permanent) completed correctly.
   - If the commit procedure succeeded, continue working with the web administration interface as needed.
   - If the commit procedure failed, the server has a software problem. Contact Avaya services.

Figure 119: Make Upgrade Permanent screen

Boot Partition screen

Figure 120: Boot Partition screen



Boot Partition screen field descriptions

The hard drive on every Avaya server reserves two partitions for system software. Use the Partition Status page for diagnostic purposes to find out the software version installed in each partition of the server's hard disk.

Additionally, you can determine which software version is currently active and which partition will become active when the server reboots.

Partition Status

To view the status of the server's hard disk partitions:

Physical Partition

This column identifies the two physical areas of the disk drive that are reserved for system software:

- Hard drive A (hda) is the only hard disk drive in the Avaya server. The server's operating system lists the partitions on the disk by device file name (for example, hda1 and hda6).
- There is no correlation between the active and inactive partitions between the two servers. For example, assume that both server 1 and server 2 are running the same software on active partition hda1. If server 2 experiences a problem and is replaced with another server, the new server could come into service running its active software on hda6. Service is not affected in any way.

Software Release

This column shows what software release is installed in each partition. The currently active software and the pre-upgrade version both appear.

Boot Partition

This column indicates whether or not the server will run this version of software when the system is next rebooted.

- For a system in service, the boot partition is normally the same as the active partition. To make the boot and active partitions match, use the Make Upgrade Permanent screen.
- If the software has not been made permanent (a software upgrade has not been completed), the status and the active partition are not the same.

Active Partition

This column shows the software that is currently active on this server.

Partition status states

The following tables show how the partition changes during a software installation.

Stable system

Before a software upgrade, the server software setup looks like this:

Partition	Software release	Reboot next from here	Currently active
1	Pre-upgrade version	yes	yes
6	Previous version (if any)	no	no

Software installed but not made permanent

This server is running the new version of software. The pre-upgrade version remains intact on the previously active partition. It is flagged as the version to run on the next reboot, in case there is a problem with the new software.

Partition	Software release	Reboot next from here	Currently active
1	Pre-upgrade version	yes	no
6	New software version	no	yes

Return to stable state

As soon as verification testing is complete, the Make Server Upgrade Permanent page commits the new software to operation. When the server reboots, it runs the new software.

Partition	Software release	Reboot next from here	Currently active
1	Pre-upgrade version	no	no
6	New software version	yes	yes

Reboot. If you click Reboot, the system performs a one-time boot to the standby partition.

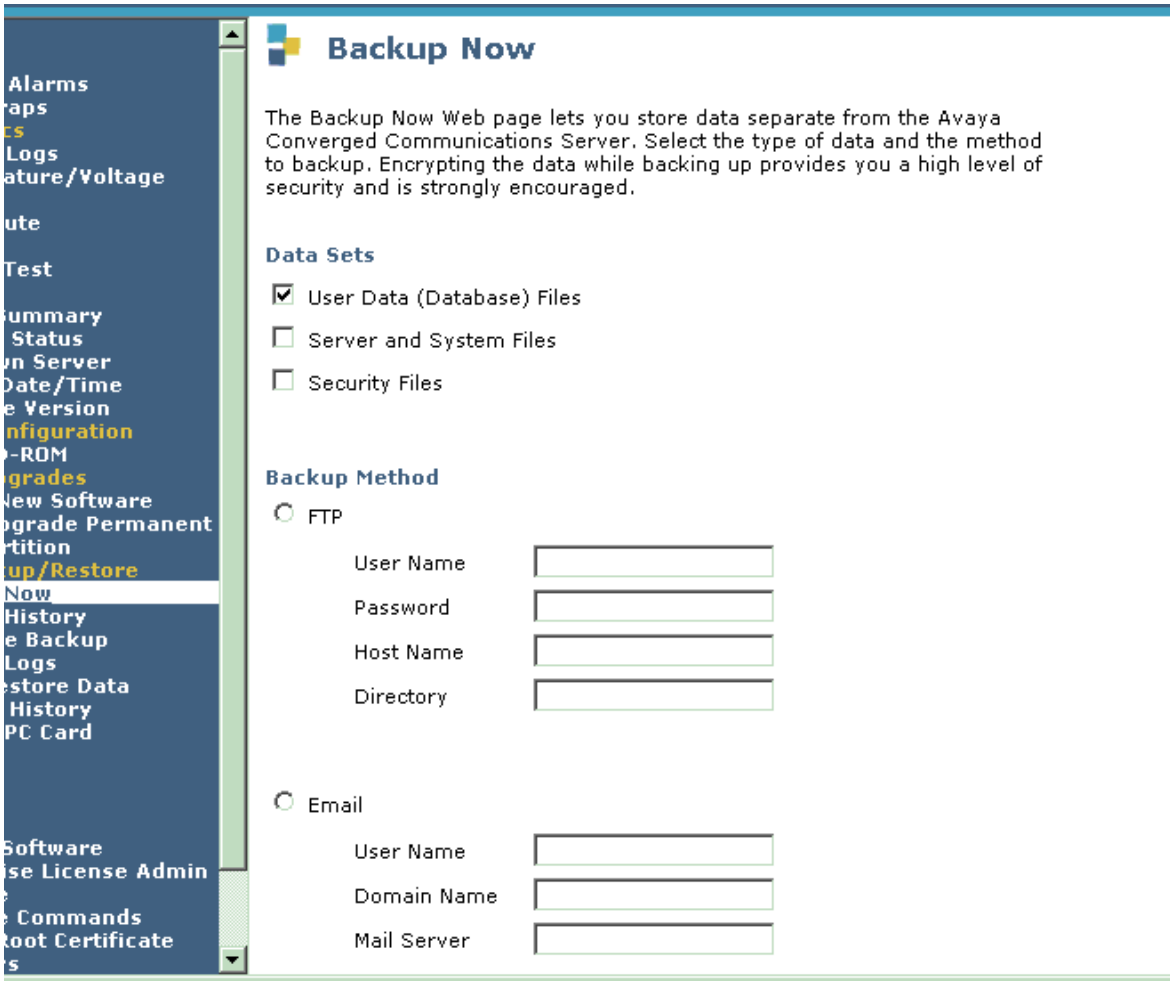
WARNING:
Switching the boot partition shuts down the server. Any translations and messages saved since the last partition switch will be lost.

Data Backup/Restore screens

Backup Now screen

Backup both the Master Administrator interface subsystem on the edge server, and the home server to back up all user data.

Figure 121: Backup Now screen



Backup Now screen field descriptions

Use this page to immediately back up system data after the server is installed. Additionally, run the backup before changing your system. This ensures that the most recent data are backed up, including new data since the last scheduled backup.

Data Sets

- **User Data (Database) Files**. Choose this selection to back up the administered information for user contacts in your system.
- **Server and System Files**. Choose this selection to back up the variable information to configure the server for a particular installation.
- **Security Files**. Choose this selection to back up the variable information to maintain security for the server.

Backup Method

- **FTP**. Choose this selection to send the backup data to an FTP server. When you choose this selection, you must also enter a user name, password, host name, and directory. The default directory for backup data on the FTP server is /var/home/ftp. If you want to use the default directory, enter a forward slash (/) in the directory field. You must start the FTP server before backing up. To enable the FTP server, see FTP Server.
- **E-mail**. Choose this selection to send the backup data as an attachment to an e-mail. When you choose this selection, you must also enter a user name, domain name, and mail server name.

  Note:

  Do not exceed the size of file your mail server can handle.

  CAUTION:

  If you choose to back up data using e-mail, the server software is unable to determine whether or not this backup method succeeds. Additionally, you cannot restore the file unless you move it to a location where it can be restored via FTP. Alternatively, you could place the e-mail attachment on the server using FTP and then restore it using the local directory option.
- **Local PC card**. Using USB flash memory for your backup files has several advantages:
  - The host server controls the flash memory. The backup process does not depend on the availability of other servers.
  - You can physically remove USB memory and place it in off site storage for safekeeping.
  - However, flash memory has limited storage space. Also, if it is not sent off site to be stored, it could easily be lost because of fire, flood, or other causes.

  Retain ____ Data Sets at Destination. Input the number of data sets you need to back up.

  Format PC Card. Flash memory must be formatted before you can store information. You only need to format once because formatting again results in losing data. You can also format flash memory using the Format PC Card screen on page 410.

Encryption

If you want to encrypt the backup data, click the box in the Encryption area of the page and enter a pass phrase using an arbitrary string of 15 to 256 characters. The pass phrase can contain any characters except the following (single quote, back slash, single backquote, quote, percent sign): **' \ & ` "%**

CAUTION:

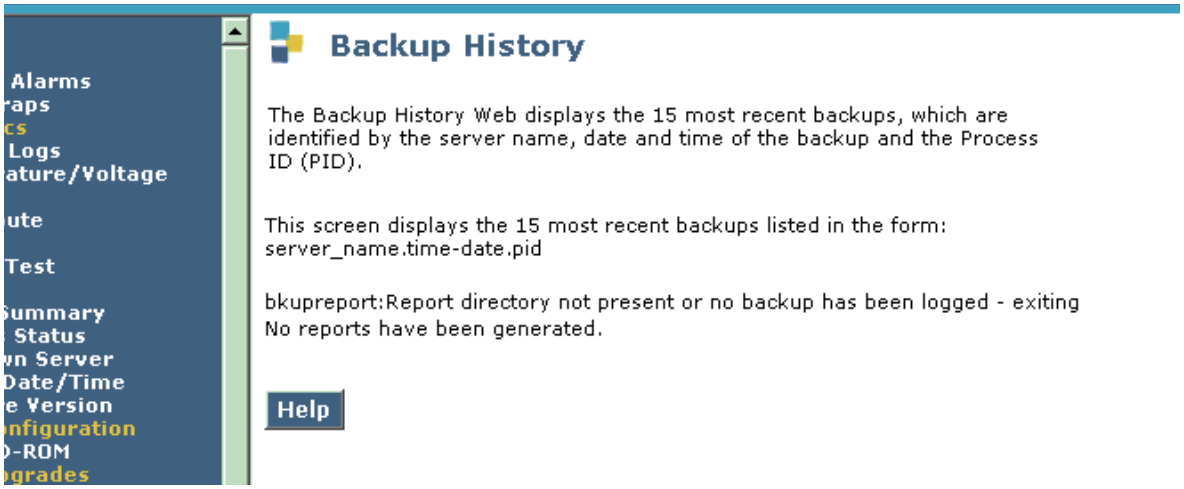
We strongly recommend that you encrypt the backup data. Create a password with a combination of letters, numbers, spaces, and special characters in the pass phrase to make it difficult to guess. You must remember the pass phrase because you cannot restore the data without it.

Click **Start Backup**. The **Backup Now** results screen displays a message indicating the backup is underway.

To check the results of the backup, click **Backup History**. The Backup History screen displays. It provides a list of the most recent data backups (15).

Backup History screen

Figure 122: Backup History screen



Backup History screen field descriptions

This page lists the 15 most recent backups.

1. Select one of the backups to review details. The following explains the parts of the backup file name:

   1 lzccs1.163608-20040719.5179

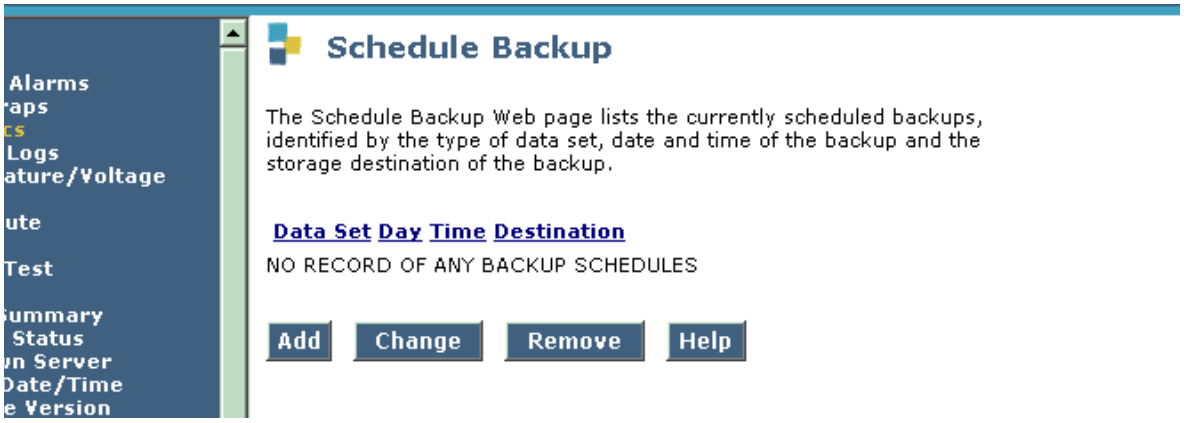
   Where lzccs1=server name, 163608-20040719=backup time (hhmmss)-date(yyyymmdd), and 5179=PID (process ID uniquely identifying this backup).

2. To review backup history, click **Check Status**.

Schedule Backup screen

When scheduling a backup, backup both the Master Administrator subsystem on the edge server and the home server to back up all user data.

Figure 123: Schedule Backup screen



Schedule Backup screen field descriptions

The backup procedure runs automatically, based on the schedule you create. Use the **Schedule Backup** screen to create and view backup schedules. From the **Schedule Backup** page, create a new backup schedule, change a backup schedule, and delete a backup schedule.

CAUTION:

When scheduling the backups, follow the general rules that apply to backup procedures. Be sure to schedule the backups to run outside of peak times when call processing on the server is at a minimum.

Data sets

The data copied during the backup procedure are the variable information used to configure the system for a particular installation. This information falls into the following three categories of data, known as data sets:

User Data (Database) Files

User data (database) files refers to data entered in the system for SIP users and associated contacts.

Server and System Files

Server and system files refers to data entered by the service technician or system administrator and used to configure the server for a particular installation, such as the server names, server IP addresses, and routing information.

Security Files

Security Files refers to data such as logon IDs, passwords or Access Security Gateway keys, firewall information, and file monitoring data bases.

Date

Year, month, and day the backup was run.

Time

Hour, minute, and second the backup was run.

Status

Shows whether the backup was successful.

Destination

Indicates how the data were recorded. It corresponds to the backup method used for the backup. Possible destinations are: FTP, e-mail, and local PC card.

Add a backup schedule

Back up both the Master Administrator subsystem on the edge server and the home server. Although you view SIP PIM data from the Master Administrator interface on the edge, those data reside on the home. Backing up the home separately assures you of having a complete data set.

Each home server needs to have it's own backup schedule created.

To create a backup schedule, you first decide what type of data you want to back up. Indicate the days and time you want the schedule to run, and the destination to which you want the backup files sent.

- To create a backup schedule:
  1. In the Add New Schedule page, select the type of data you want to back up by selecting the appropriate data set.
     - If backups are already scheduled, the page lists the current backup schedules. Look at it carefully to determine what backup schedule you want to add.
     - If this is the first backup schedule to be created, the **Schedule Backup** page displays a message that there is no record of any backup schedule.
  2. Select a backup method to indicate the destination to which the system sends the backup data.
  3. If you selected local PC card as your backup method, indicate how many copies of the selected data sets you want to retain by entering a value in the small text box at the bottom of the **Backup Method** area of the page. We recommend that you retain two copies of all data sets selected for backup.
  4. If you want to encrypt the backup data, click the box in the Encryption area of the page and enter a pass phrase using an arbitrary string of 15 to 256 characters.

     SECURITY ALERT:
     We strongly recommend that you encrypt the backup data. You must remember the pass phrase because you cannot restore the data without it.
  5. Select the days of the week by clicking the appropriate check boxes, and select the hour and minute you want the backup procedure to start by selecting a time from the drop-down boxes. You can select multiple days but only one time for the backup schedule to run.
- Click Add New Schedule to save the schedule you just created.
- The system displays the **Schedule Backup** page, which adds the new backup schedule to the bottom of the schedule list.

Change a backup schedule

You can change the days and time an existing backup schedule runs. You can also change the destination to which the system sends the backup data.

Backup both the Master Administrator interface subsystem on the edge server and the home server to back up all user data, including SIP PIM data.

1. On the **Schedule Backup** screen, select the radio button next to the backup schedule you want to change.
2. Click Change at the bottom of the page.

   The **Change Current Schedule** screen displays the information for the backup schedule you selected in Step 1.
3. Make the changes you want to the backup schedule.
4. Click **Change Backup Schedule** to save the schedule you just created.

The system displays the **Schedule Backup** page, which lists the changed backup schedule.

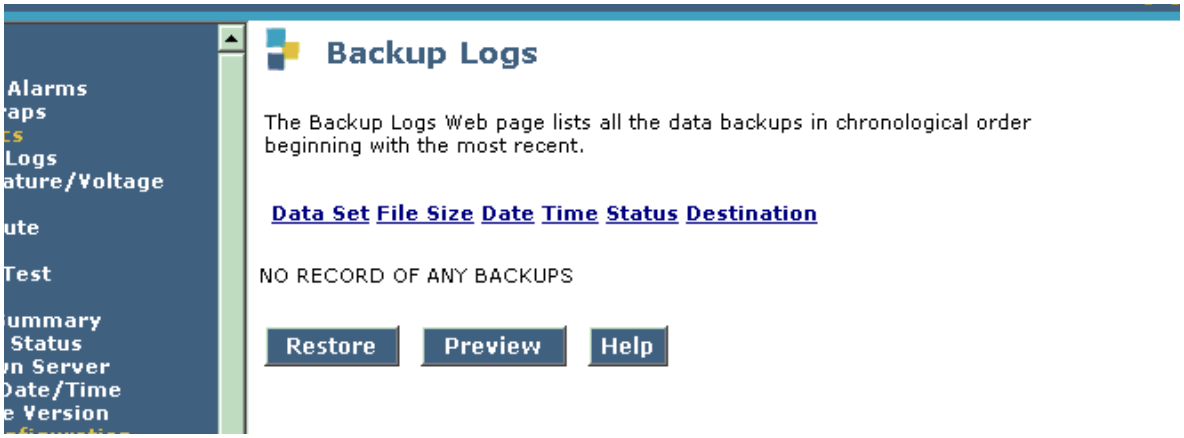
Remove a backup schedule

To delete an existing backup schedule:

1. On the **Schedule Backup** page, click the radio button next to the backup schedule you want to delete.
2. Click **Remove** at the bottom of the page. The backup schedule you deleted is removed from the list displayed in the **Schedule Backup** page.

Backup Logs screen

Figure 124: Backup Logs screen



Backup Logs screen field descriptions

When you back up data, the system creates an image as a tape archive file that contains information, such as what data sets were backed up, whether or not the backup was successful, and how the data were recorded. Use this page to view a log of backup images for all the backups you have run. If appropriate, you can then restore the corresponding backup data.

Data Set

Indicates what data were recorded. Possible sets are: User Data (Database) Files, Server and System Files, and Security Files.

File Size

Physical size of the backup file.

Date

Year, month, and day the backup was run.

Time

Hour, minute, and second the backup was run.

Status

Shows whether the backup was successful.

Destination

Indicates how the data were recorded. It corresponds to the backup method used for the backup. Possible destinations are: FTP, e-mail, and local PC card.

Steps to preview or restore backup data

Click one of the following buttons:

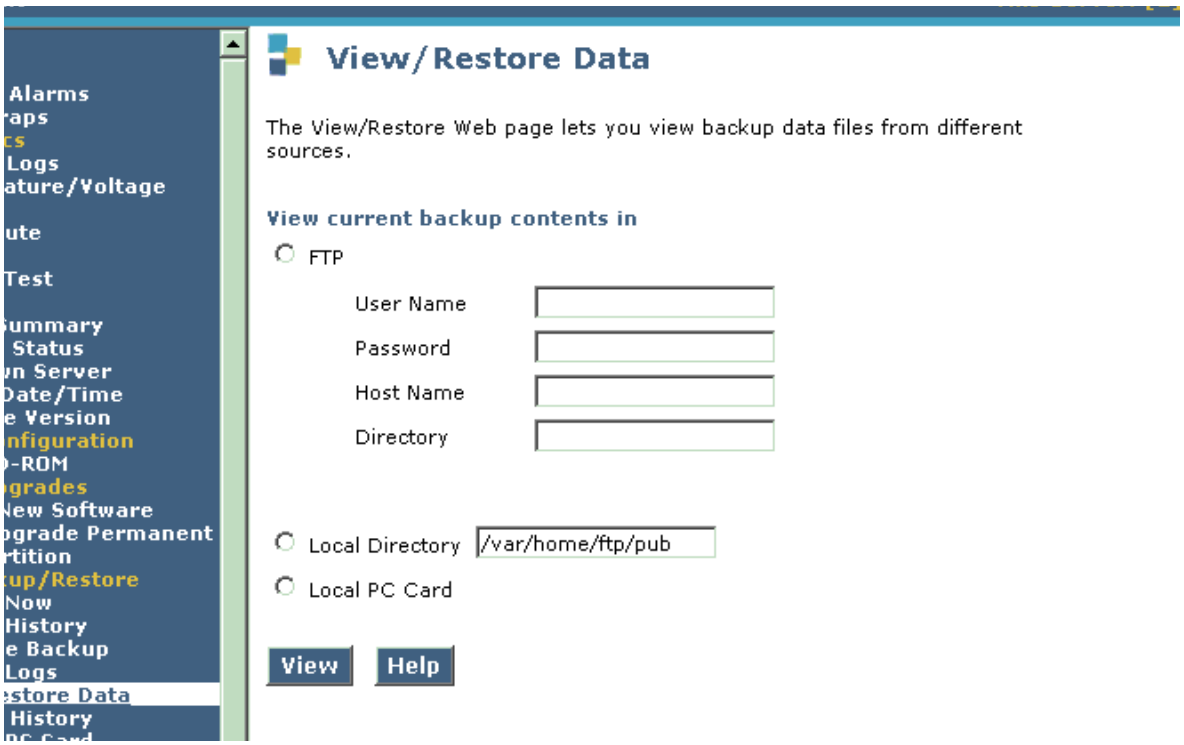
1. Scan the log until you see a backup image to preview or restore. Select it by clicking the radio button to the left of the image.
2. If no entries exist in the backup log, you will see a message that there is no record of any backups.
3. Click one of the following buttons:
   - **Preview**. Use the Preview button if you are not sure you have selected the correct backup image. When you click Preview, the system displays a brief description of the data associated with the backup image.
   - **Restore**. When you click Restore, the system displays more detailed information about the backup image you selected and then displays a page that tells you whether or not the restore procedure is successful.

You must select a backup image before you click Preview or Restore, or an error message appears. To clear it, simply click the browser's Back button, then select a backup image to preview or restore.

If the data you want to restore were backed up using e-mail, or if the data were backed up using FTP but the FTP server does not allow reading, the file to be restored must first be copied to this server with FTP or with a download function. Once the file is copied to this server, it can be restored.

View/Restore Data screen

Figure 125: View/Restore Data screen



View/Restore Data screen field descriptions

If your system malfunctions and you lose data, the saved data from the backup can restart the system. Copy the data to the server from the location where saved. Restore a backup image, which is a tape archive (tar) file that contains backed-up data.

FTP

Before the FTP server transfers the backup image, the media server must first log on to the FTP server. You must therefore also enter the following information:

User name. Enter the name **anonymous** if you are using an anonymous account. Otherwise, enter your real user name.

Password. If you are using an anonymous account, you will typically enter your e-mail address as the password. However, you should check with the FTP server administrator to verify this. If you are not using an anonymous account, enter your real password.

Host name. Enter the DNS name or IP address of the FTP server on which the data were backed up. Use the dotted decimal notation to enter IP addresses (for example, 192.11.13.6).

Directory. Enter the path name for the directory in which the data are stored on the FTP server. Contact the FTP server administrator if you have questions.

Local directory

Choose this selection if you know the backup image was saved to a local directory. You must enter the path name for the directory. The default directory is /var/home/ftp/pub.

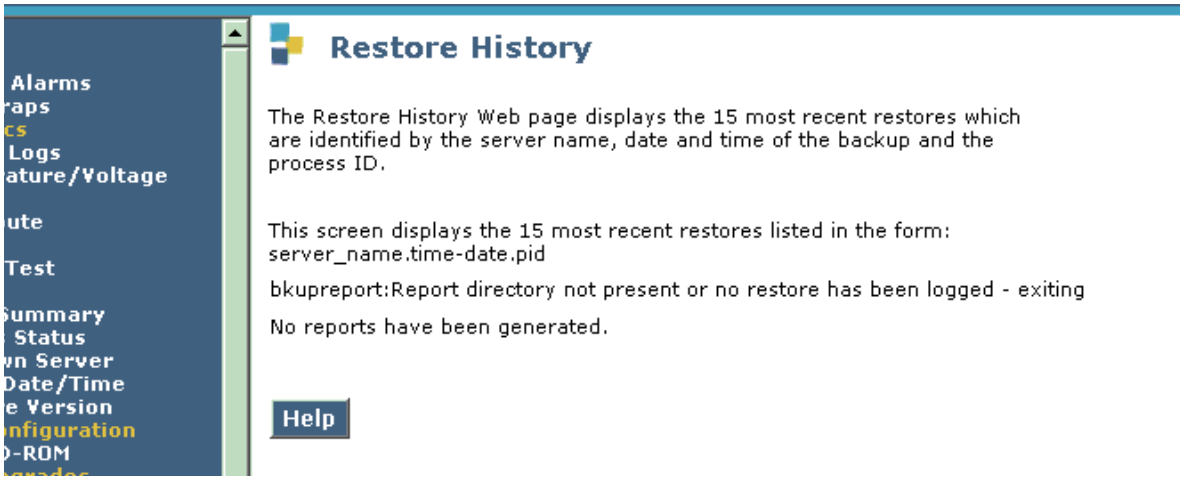
Local PC card

Using USB flash memory for your backup files has several advantages:

- The media server controls the flash memory, therefore, the backup process does not depend on other available and accessible servers.
- You can physically remove USB flash memory for off site storage safekeeping.
- However, flash memory has limited storage space. Also, if it is not sent off site to be stored, it could easily be lost because of fire, flood, or other causes.
- Click **View** to ensure the correct backup image is selected.
- Click **Restore** to begin. The system displays a View/Restore Data results page indicating whether the restore procedure is successful.

Restore History screen

Figure 126: Restore History screen



Restore History screen field descriptions

This page lists the 15 most recent restores.

1. Select one of the restores to review details. The following explains the parts of the restore file name:

   1 lzccs1.163608-20040719.5179

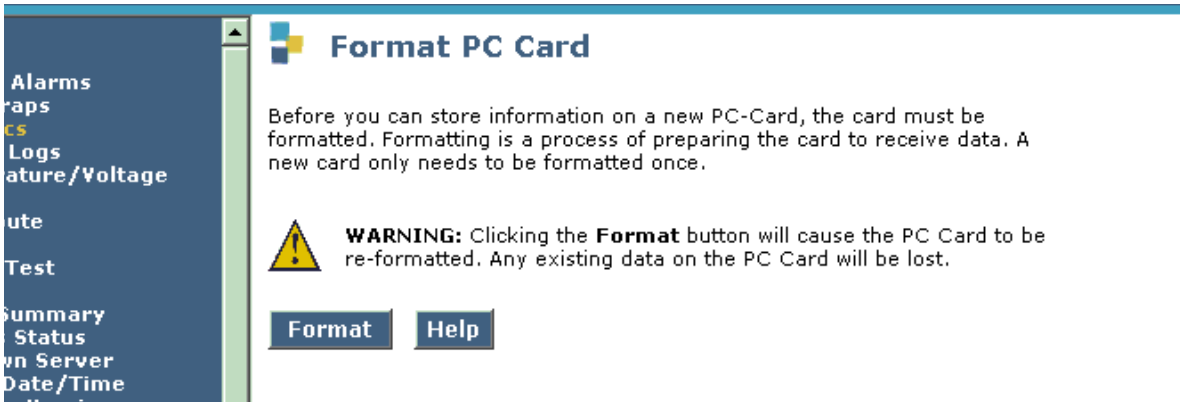
   Where lzccs1=server name, 163608-20040719=backup time (hhmmss)-date(yyyymmdd), and 5179=PID (process ID uniquely identifying this backup).

2. To review restore history, click **Check Status**.

Format PC Card screen

Flash memory must be formatted before you can store information. New memory requires only one format. Used flash memory that contains data is erased if you format it again. Click **Format**. You are prompted whether you want to format. Click **Yes** to continue with the format. Note that you may also format the flash memory in conjunction with the Backup Now screen on page 397.

Figure 127: Format PC Card screen



Format PC Card results screen

The results of your PC card format displays.

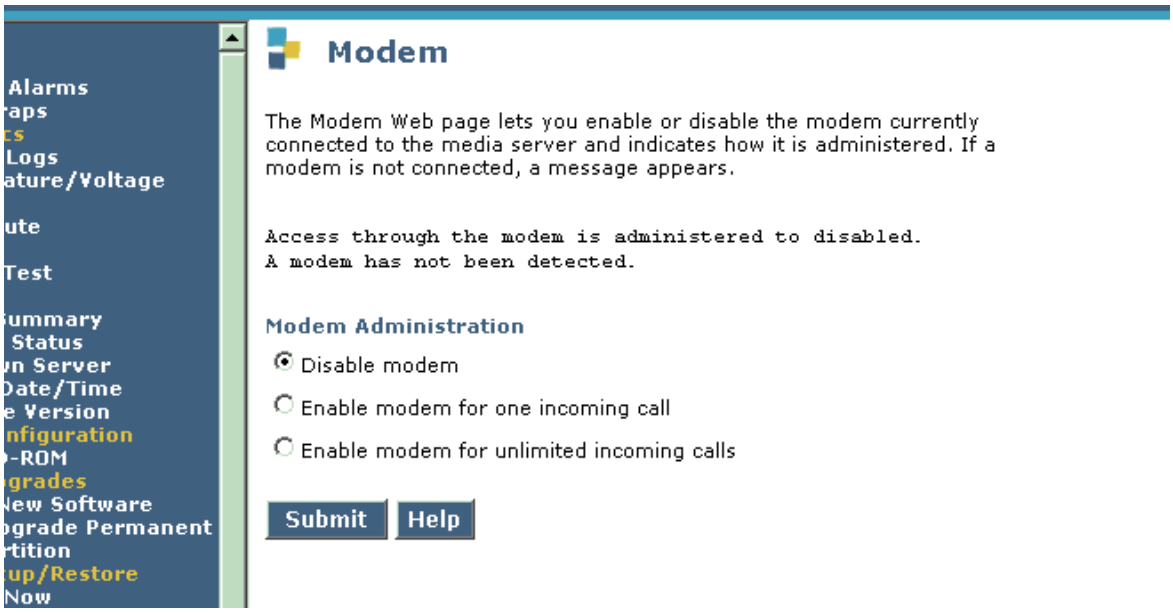
Security screens

This section discusses the following security screens:

Modem screen

Use the Modem page to allow the server's modem to accept one, unlimited, or no incoming calls. The call-receiving status of the modem can be changed to control access to the Avaya server.

Figure 128: Modem screen



Modem screen field descriptions

Modem Administration

To check or change the call-receiving status of this server's modem:

- **Disable modem**. Choose this option to prevent all incoming calls. The modem can still report server alarms, but no one can dial in on this line.
- **Enable modem for one incoming call**. Choose this option to allow only one incoming call. This option is typically used before a remote services procedure is done at a site where the modem is usually disabled for incoming calls.
- **Enable modem for unlimited incoming calls**. Choose this option to allow unlimited incoming calls. The modem is available to support remote services personnel, provided they know the correct access information.

To select one of the options, click **Submit**.

Solving modem problems

Modem problems:

1. No modem found - modem access disabled.

   The modem for this server is not installed or has been disconnected. Connect the modem and try again.

2. Modem currently in use - try again later.

   The modem is currently engaged in a call. Do the following:

   - Try this operation again. If one of the servers was reporting an alarm, the line should be clear.
   - If the line is busy, find out who is using the modem. If Services personnel are logged in, the line could be busy for some time. However, ensure that an authorized user is using the line.

3. Modem NOT enabled - error. This message can occur if you try to enable the modem to accept unlimited incoming calls if the `mgetty` program (the process in charge of the modem) does not start.

   To solve this:

4. Wait a few seconds, click Enable/Disable Modem on the main web administration menu to see if the mgetty process is running.
5. If a **modem access set for multiple calls but currently disabled** message appears, the mgetty process is still not running. Go to 2.
6. If no error message appears, select Enable for unlimited incoming calls.
7. Disable the modem, select Enable for unlimited incoming calls.

   - If the **modem NOT enabled - error** message appears again, there is a serious problem. The system should be examined by services personnel.
   - Modem access set for multiple calls but currently disabled. The mgetty (modem program) process is not running, although the server has been set to accept unlimited incoming calls. To solve this, follow the same steps as for **modem NOT enabled - error** above.

FTP screen

Use the FTP page to activate file transfer protocol (FTP) service on the Avaya server. Activate this service for an FTP application that resides on another computer or server for which you want to transfer files to or from the Avaya server.

CAUTION:

To keep your Avaya server secure, always deactivate FTP service when your file transfers are complete. When you deactivate FTP service unauthorized users cannot use FTP to transfer files to or from the Avaya server.

Figure 129: FTP screen

Steps to Start or Stop FTP service

To start or stop FTP service:

1. The FTP Server page shows the current state of FTP service: enabled or disabled. Normally FTP service is disabled between file transfers.
2. If service is enabled and you need to transfer files, continue to step 5. Otherwise, secure the server against potentially unauthorized files transfers as follows:
   - Click **Stop Server** to deactivate FTP service on the Avaya server. The FTP Server page shows a new status of disabled. You can continue working with the web administration interface as needed.
3. If service is disabled and you need to transfer files:
4. Click **Start Server** to activate FTP service on the Avaya media server. The FTP Server page shows a new status of enabled.

5. On the computer or server that contains the files to copy, transfer files to the Avaya server as follows (see Copy files using FTP for details):
   - Open an FTP application on your computer (run FTP or open a GUI FTP application).
   - Log on as anonymous, with your e-mail address as your password.
   - Set mode to binary, then put the correct files on the Avaya media server.
   - When you finish, close the FTP application.
   - When file transfer is complete, click the web administration interface window to access the FTP Server page.
   - Click **Stop Server** to deactivate FTP service. This prevents unauthorized users from transferring files to or from the Avaya server using FTP.

FTP operation

The FTP service operates on the Avaya media server as follows:

- Files are transferred to the /var/home/ftp subdirectory on the server. Files (such as keys.install files) may also be copied to the /tmp subdirectory.
- FTP service is normally available on the services and corporate LAN interfaces. However, FTP service to the corporate LAN interface may be blocked as follows:
  - On the main menu under Security, click the Firewall link. When the page appears, note the setting for the FTP service on port 21.
  - If FTP service is disabled (the check box is clear), devices that connect to the Avaya server across the corporate network interface cannot use their FTP applications to transfer files to or from the server. However, a laptop connected to the services interface should still be able to transfer files using its FTP client application.
  - If FTP service is enabled (the box is checked), devices that connect to the Avaya server across the corporate network interface can use their FTP client applications to transfer files to or from the server.
  - If you change the FTP setting, click **Set Security**. Review the page when it refreshes to ensure that changes were made correctly.

Copy files using FTP

Use this procedure to copy (put) files onto the Avaya server using an FTP application on your computer. Typical files to transfer include new license or authentication files, firmware upgrades, system announcements, or keys.install files that may be used with network time servers.

Prerequisites

To use this page, FTP service must be available for the Ethernet interface you are using. Occasionally this service may be blocked on the customer LAN interface for security reasons (see Set LAN Security) FTP service must be enabled on the FTP Server page.

Transfer procedure

To copy files to the server using an FTP application on your computer:

1. Log on to the Avaya server.
2. On the main menu under the Security section, click Start/Stop FTP Server.
3. Check the current state of FTP service: enabled or disabled. FTP service should be disabled between file transfers.
4. Click Start Server to activate FTP service on the Avaya server.

   SECURITY ALERT:
   You cannot start FTP service if it is blocked on the Firewall page.
5. On the computer or server that contains the files to copy, run an FTP application.
6. You can use a GUI FTP application if one is installed on your computer. Alternatively, you could run a command-line version of FTP. For example:
   - From the Start menu on a Windows system, select Run.
   - In the Run window, type ftp <hostname or IP address> at the prompt.

   Note:
   You can only enter the server name instead of an IP address if you are accessing the server over a network with DNS service. Direct connections using a laptop (the services link) must use the server's IP address if DNS is disabled.
7. Specify the following to connect to the Avaya server:
   - Host name: the name or the IP address of the media server
   - User ID: anonymous
   - Password: your e-mail address
   - Terminal type: the appropriate type for your computer if prompted
8. Set mode to binary as follows:
   - In the FTP application window, select the Binary option.
   - For a command-line session, type **bin** at the prompt.

9. Put the files onto the server.
   - In the FTP application window, choose the correct files and copy them as required by your application.
   - For a command-line session, type **put </directory/filename>** at the prompt for each file you need to copy, where </directory/filename> is the location of the file on your computer. Files are always placed in the /var/home/ftp subdirectory on the server.

   Note:

   For a Windows system, you may need to preface the put destination with a drive letter. For example, **put <drive:\directory\filename>**. Note that Linux systems use forward slashes in the directory name.

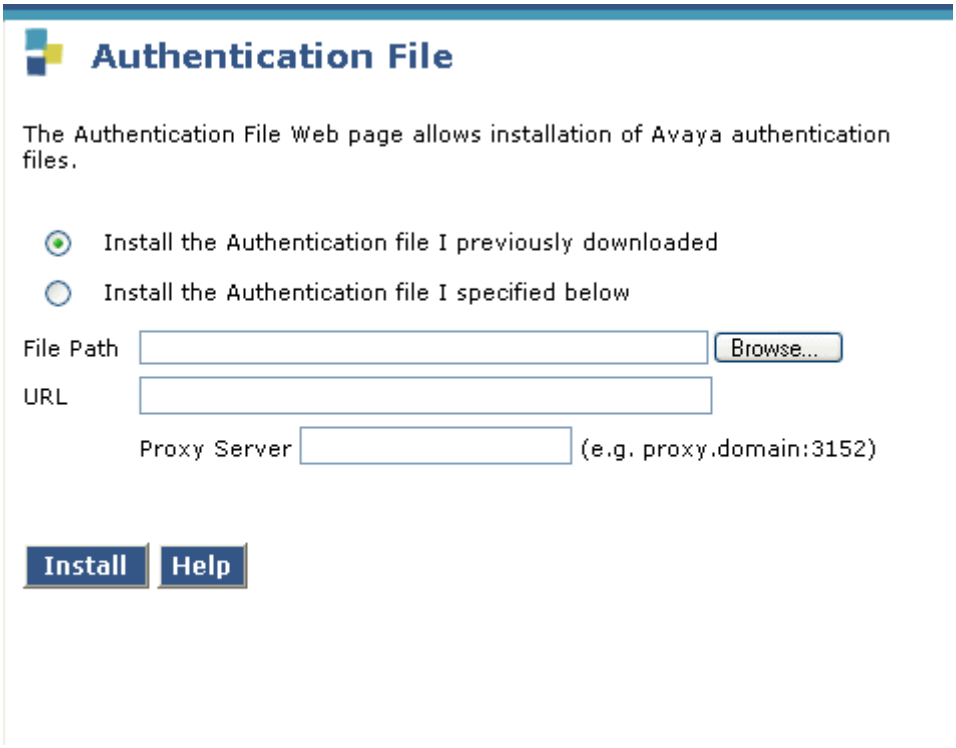
10. When the file transfer is complete:
    - Close the FTP application window.
    - For a command-line session, type **quit**.
11. Disable FTP service on the Avaya media server to prevent unauthorized users from transferring files there:
    - Click on the Avaya server's web interface window to access the Start/Stop FTP screen.
    - Click **Stop Server** to deactivate FTP service.

Authentication File screen

At install time, the installer probably downloaded the authentication file to the directory `/var/home/ftp/pub` on the SES server. If the authentication file is there, choose the first radio button, **Install the Authentication file I previously downloaded**.

If the authentication file is on the local network, specify the path to the file's location. Choose the second radio button, **Install the Authentication file I specified below button**, and then select Install. Specify a URL and proxy server if the file is on a remote network.

Figure 130: Authentication File screen



Authentication File screen field descriptions

File Path

Only enter data in this field if you choose the second radio button. This field specifies the file path to the authentication file that is not typical for a SES system.

URL

Only enter data in this field if you choose the second radio button.

Enter the URL where the authentication file resides.

Proxy Server

Only enter data in this field if you choose the second radio button.

If you need to specify a proxy server to the URL entered above, name that server here.

Authentication File screen commands

Install the Authentication file I previously downloaded

If you select this radio button, do not type any information in the fields below. The SES system has a record of the location of the authentication file.

Install the Authentication file I specify below

If you select this radio button, fill either the **Path** field, or the **URL** and **Proxy Server** fields to indicate where the authentication field resides. You may not need to specify a Proxy server, depending on your situation

Install

Submit the information.

Firewall screen

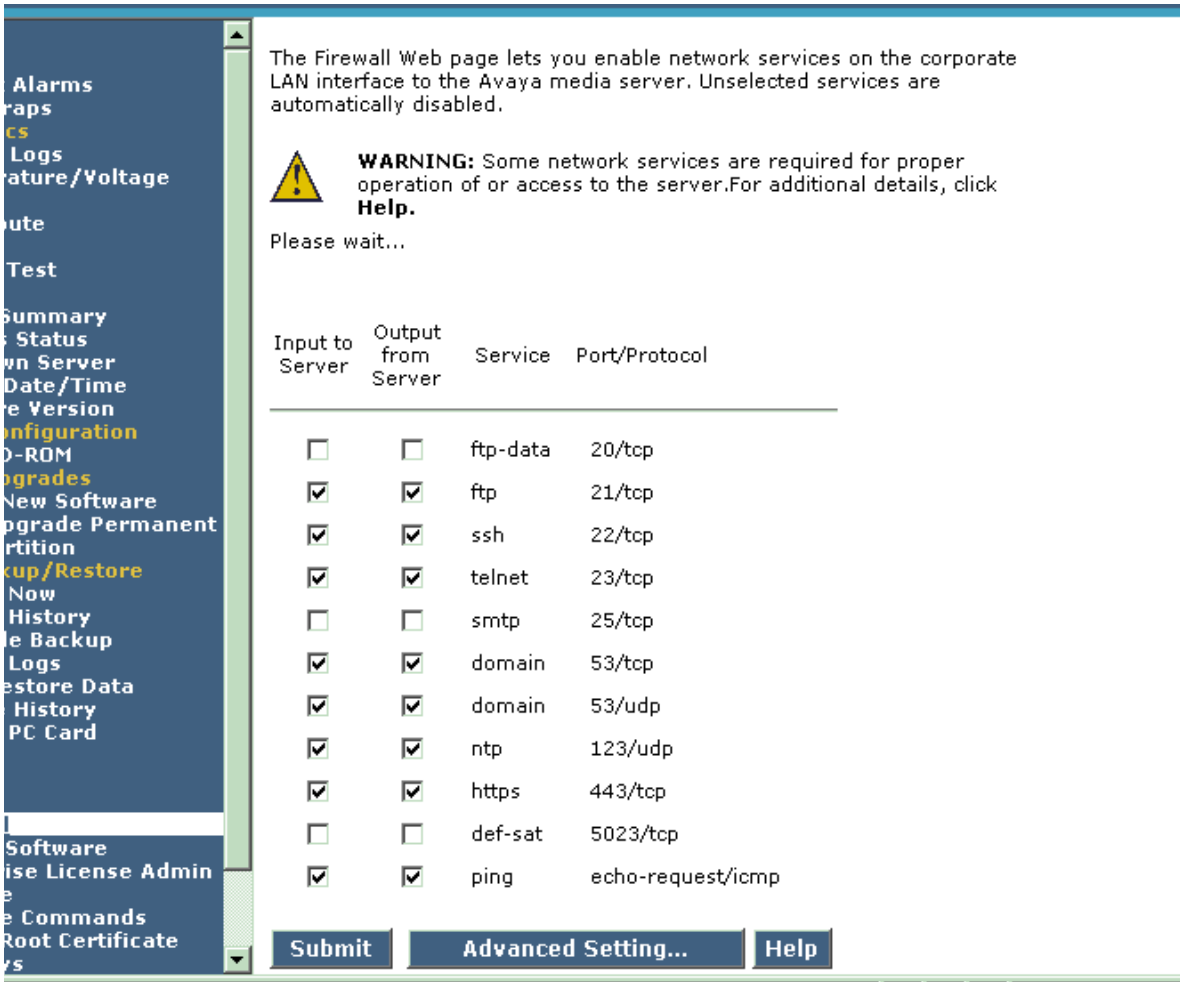
Use the Firewall page to enable or disable network services on the corporate LAN interface to the Avaya server. You can activate or deactivate these services as needed to control features or access to the server. Your changes to this interface do not affect services on the other Ethernet interfaces.

This page is a front-end to the standard Linux command ipchains. Ipchains is used to set up, maintain, and inspect the IP firewall rules in the Linux kernel. These rules can be divided into four categories: the IP input chain, the IP output chain, the IP forwarding chain, and user-defined chains. This page only allows administration of the input chain. The output chain and forwarding chain are set to the value **accept**. There is no user-defined chain.

CAUTION:

The IP services that are checked on the Firewall page are already enabled. To disable IP services, you must deselect the service. Be careful about disabling common IP services, it may adversely affect your Avaya server.

Figure 131: Firewall screen



Firewall screen field descriptions

Input to server

The IP service you select for incoming server communications. This selection can be different from outgoing server communications.

Output from server

The IP service you select for outgoing server communications. This can be different from incoming server communications.

Service

A list of names of the most commonly used IP services. Their current status is shown: either enabled (checked) or disabled (check box clear). These are standard Linux services. For details on their operation and use, refer to published Linux documentation.

FTP-data: Used with FTP. One channel controls the connection to transfer data, and the other channel controls the data transfer.

File Transfer Protocol (FTP): Used for uploading or downloading data files, announcements, license files, or firmware.

Secure shell (SSH): A secure shell (SSH) remote interface utility can be used as an alternative to telnet. SSH commands and passwords are encrypted, and both ends of the client/server connection are authenticated through a digital certificate. The SSH suite includes a secure copy (SCP) program that can be used as an alternative to FTP. The SSH and SCP utilities provide greater security than FTP and telnet, and should be used if available.

Telecommunications network (telnet): provides a command-line interface for running server platform commands and applications such as SAT.

Simple Mail Transfer Protocol (SMTP): supports e-mail service across the web.

Domain Name Service (DNS): runs on port 53/tcp and 53/udp. The server uses DNS to resolve host names. For example, if you back up to an FTP server and name it, the port must be open for the server to execute a DNS query to find the IP address of the server name.

Network Time Protocol (NTP): allows the media server to synchronize its time with an external time source.

Secure Hypertext Transport Protocol (HTTPS): A secure extension to HTTP that encrypts all messages between the web server and a browser. It also uses a digital signature to authenticate users and servers.

Ping: permits any ICMP requests to be echoed back. You have the option to select this common service.

Port/Protocol

This column shows what port on the Ethernet interface this service uses, and what protocol it uses. This column shows what port on the Ethernet interface this service uses, and what protocol it uses. Common protocols include Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

To check or change the services that are allowed on the corporate LAN Ethernet interface:

- To disable an IP service:

  Clear the check box to disable this service on the corporate LAN interface.

- To enable an IP service:

  Check the box to activate a service on the corporate LAN interface.

- To view all IP services:

  Click Advanced Setting to adjust the status of a service that is not listed on the first page. The system redisplays this page, listing all the Linux IP services available for this Ethernet interface.

  CAUTION:

  The changes you input on the basic settings page are erased when you click and move forward to the Advanced Setting Web page.

WebLM Software screen

Use this screen to view whether WebLM is currently enabled on this server and to enable or disable it.

WebLM does not automatically download license files from an RFA server. At installation, the installer accesses the RFA web site with the laptop, downloads a license file, and then installs it on the server. See Chapter 7: Installation procedures on page 67.

Figure 132: WebLM screen

WebLM Software screen field descriptions

You have the flexibility to manage features and capacities among all SES hosts by enabling WebLM Software.

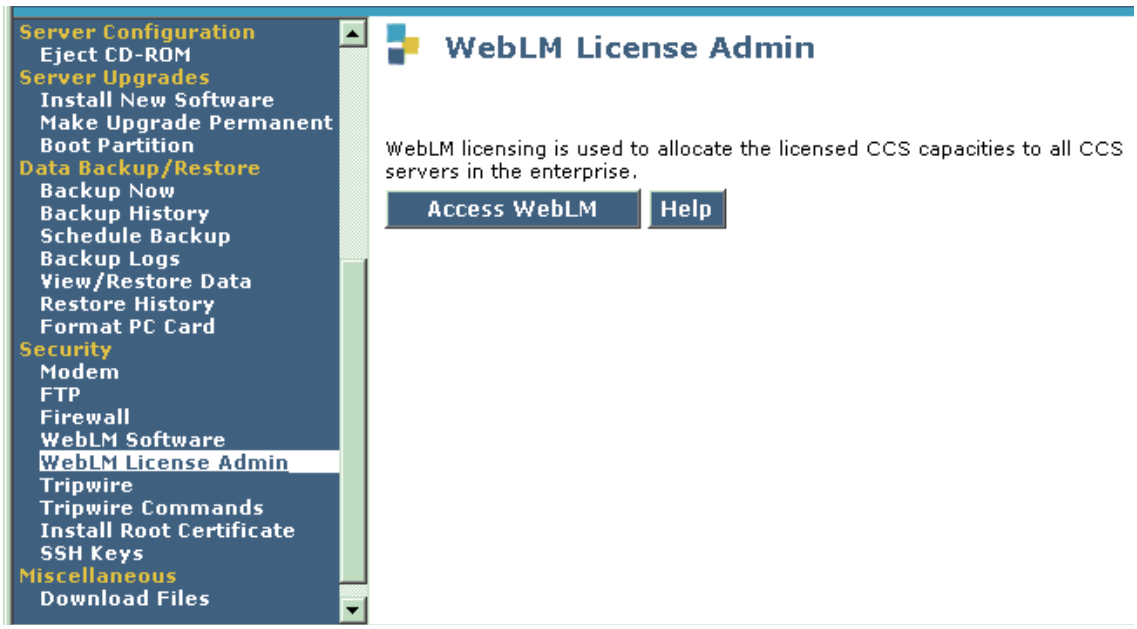
WebLM License File

Before you enable a media server, a valid master enterprise license file is required, which is generated by the Remote Feature Activation (RFA). WebLM Software enforces and defines the capacity limits of the server and sends them to the master enterprise license file.

Understand that the license expiration date is verified when installing WebLM software. The date generated by the license file must not be pre-dated to the current date of the WebLM server. (This can happen due to time-zone differences between RFA and the WebLM server.)

WebLM License Admin screen

Figure 133: WebLM Licence Admin screen



WebLM License Admin field descriptions

Select **Access WebLM** to view the WebLM application.

WebLM License File

WebLM is a tool that enforces and defines the capacity limits of an Avaya server to the license file, which is generated by the Remote Feature Activation (RFA). The capacity limits are then allocated to the individual Avaya servers using license files.

CAUTION:

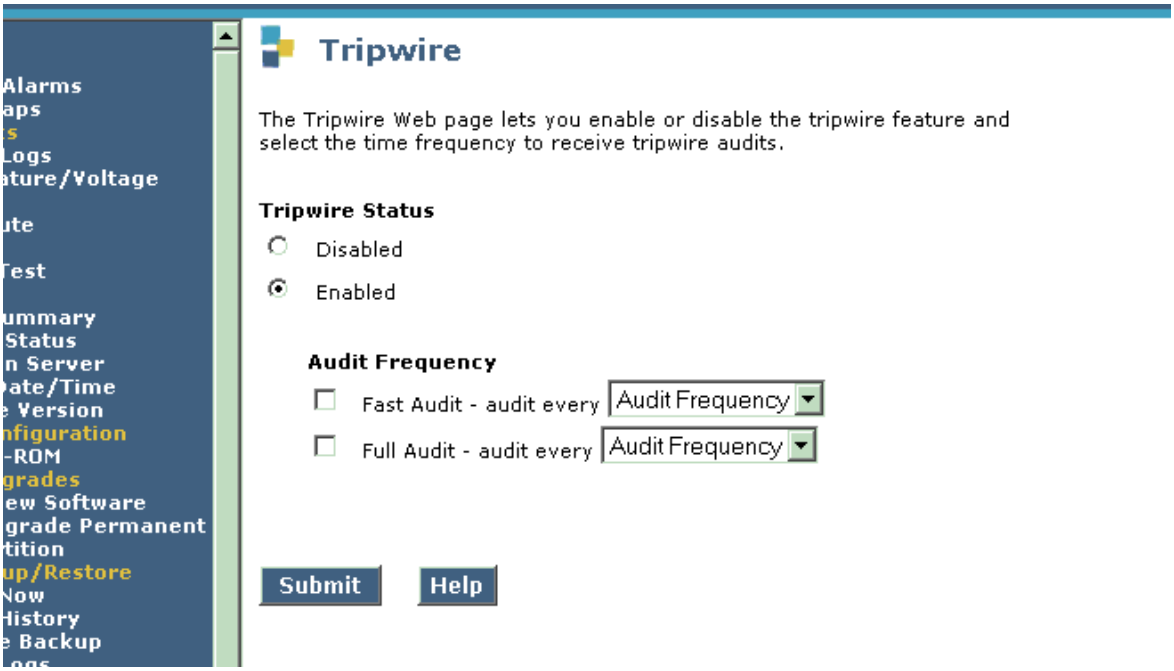
You can not exceed the limit defined in the WebLM license file. If you want to add an edge or basic proxy to a server, and all instances in the license file are already allocated to other servers, you must first generate and then upload a new WebLM license file via RFA.

WebLM displays the following information of the Avaya servers within the SES system:

- Enterprise SID
- System IDs and Module IDs of the servers
- Expiration date of master enterprise license file. For the initial release of EWL the expiration date is set to 01/01/9999, which means it never expires.
- Applications covered by the master enterprise license file.
- Enterprise feature values and capacities.
- Allocation License Duration. Each allocation license file has an expiration date based on the current date plus the license duration.

Tripwire screen

Figure 134: Tripwire screen



Tripwire screen field descriptions

Tripwire Status

Disabled

If tripwire is disabled, a status message informs you.

Enabled

If Tripwire is enabled and a signature database does not exist, another web page prompts you to add a tripwire database.

1. To add a tripwire database, click **Yes**. If you select No, a page appears indicating the tripwire is disabled and a signature database will not be created.
2. If tripwire is enabled, a status indicates tripwire is enabled with Fast Audit and frequency, Full Audit and frequency, or both.

Audit Frequency

Fast Audit

- Scheduled to run every 15 minutes, 30 minutes, 1 hour, 2 hours, 4 hours, 8 hours and 12 hours.
- A cron job is created in /etc/cron.d.
- Audits that run at 15 and 30 minute intervals are started on the .-hour, for example: *:00, *:15, *:30, and *:45 for 15 minute intervals and *:00 and *:30 for 30 minute intervals. The audit does not begin immediately but starts at the next time interval hourly, quarterly, half-past, or three-quarters past the hour
- Hourly audits are run at 3 minutes past the hour (for example: 12:03) as specified in twcron.
- Scheduled to run hourly, daily, or weekly. When a full audit is scheduled a cron job is created in /etc/cron.daily, /etc/cron.hourly, or /etc/cron.weekly depending on the standard time selected. It is run at the time specified in /etc/crontab for the corresponding frequency.

Full Audit

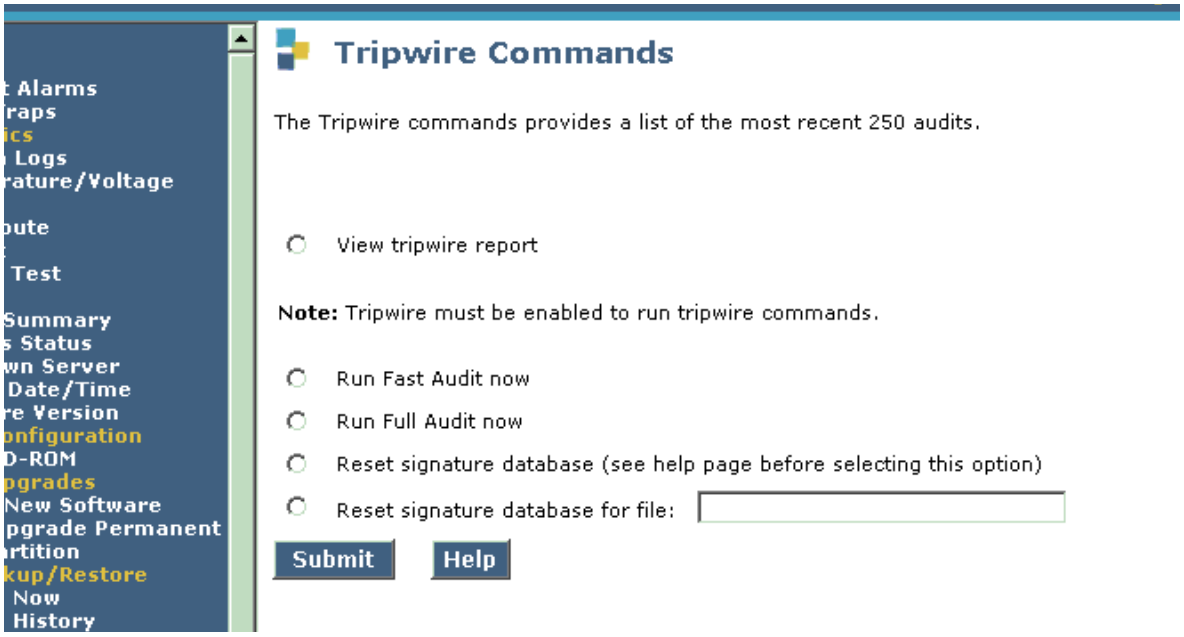
The standard times are:

- hourly jobs: one minute past the hour, for example, 12:01
- daily jobs: 4:02 a.m.
- weekly jobs: 4:22 a.m. on Sundays

To submit your selection, click **Submit**.

Tripwire Commands screen

Figure 135: Tripwire Commands screen



This page provides a list of tripwire audit reports (if Tripwire is enabled on the server) with the most recent 250 audits. Select one of the audit reports to review its details. Click **Submit**.

The following explains the parts of a tripwire audit report:

baccarat2-20030111-0416213.twr

Where server name=baccarat2-date the server is audited (yyyymmdd)-time the server is audited (hhmmss), and .twr identifies the report as a tripwire audit report

If tripwire is disabled, the following command appears: **View tripwire report**

To submit your selection, click **Submit**.

Install Root Certificate screen

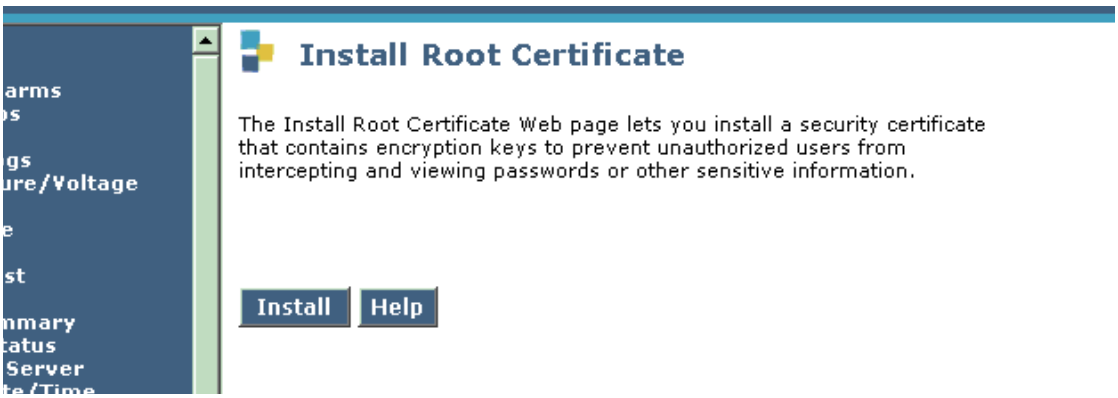
Use the Install page to install an Avaya root certificate on your computer to establish Avaya Inc. as a trusted Certificate Authority (CA). See Security certificates overview for details. First click **Install**.

Internet Explorer Steps

Follow these steps:

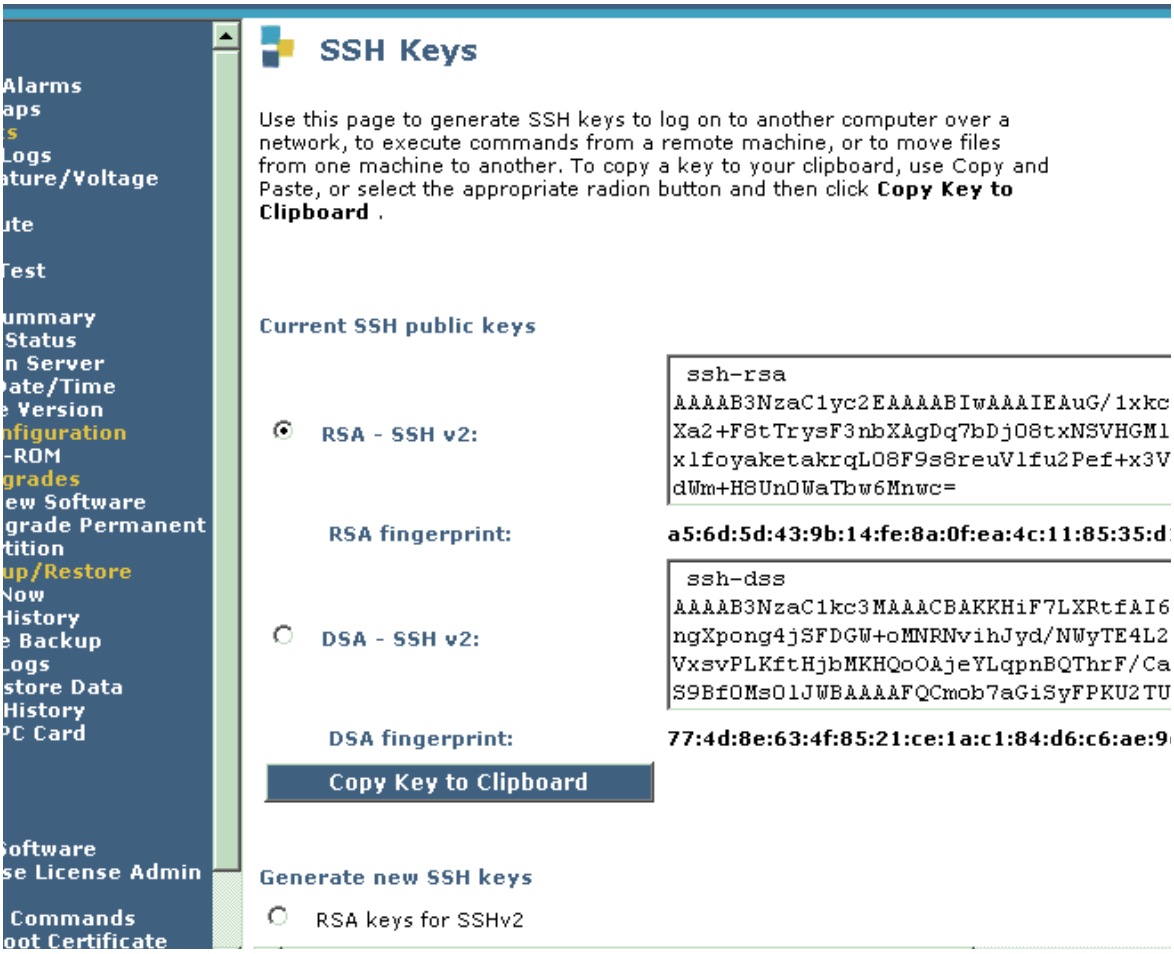
1. From the File Download dialog box, click **Open**. Do not save this file to disk!
2. From the Certificate dialog box, under General tab, click **Install Certificate**.
3. The Certificate Manager Import Wizard guides you through the process. Accept all default values. On the final page, wait for the install to complete, click **Finish**.
4. A Root Certificate Store message may appear. Click **Yes** to add the certificate to the Trusted Root Certification Authorities store.

Figure 136: Install Root Certificate screen



SSH Keys screen

Figure 137: SSH Keys screen



SSH Keys screen field descriptions

Secure Shell is a security program to log in to another computer over a network, to execute commands from a remote machine, and to move files from one machine to another. The program features authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist.

When using ssh's slogin (instead of rlogin) the entire logon session, including transmission of password, is encrypted. Because of this, it is almost impossible for an outsider to collect passwords.

Current SSH public keys

The keys currently installed on your computer are displayed.

Generate New SSH Keys

To generate new SSH keys, make a selection, and click Generate SSH Keys.

- RSA keys for SSHv2
- DSA keys for SSHv2

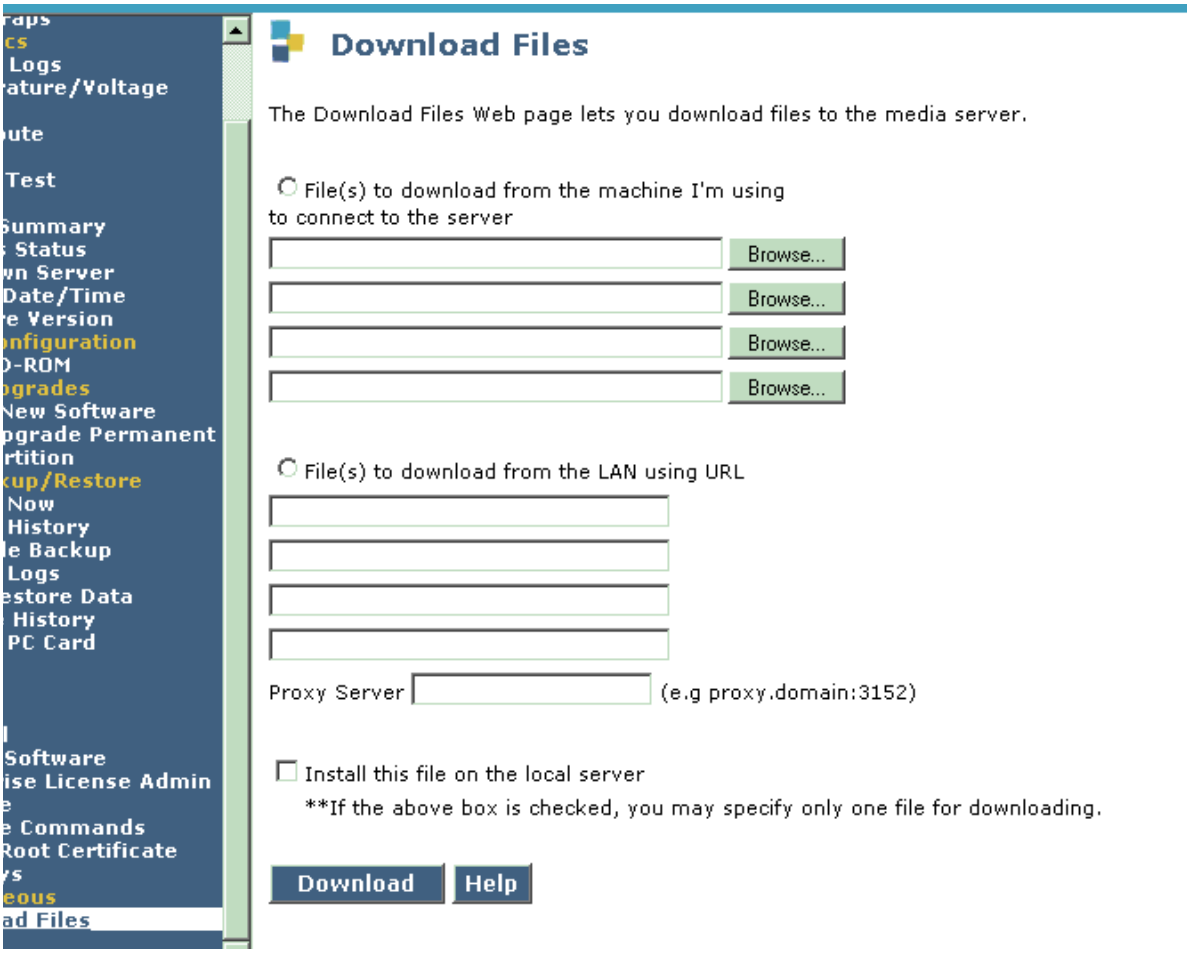
For more information about SSH, visit: http://www.ssh.com

Miscellaneous screen

Download Files screen

Use the page to download files onto the Avaya server from another server across the network using HTTP protocol. Typical files to download include new license or authentication files, firmware upgrades, or keys.install files, all which may be used with network time servers.

Figure 138: Download Files screen



Download Files screen field descriptions

Prerequisites

To use the Download page, the server must be able to access the:

- Corporate LAN (and typically its DNS server) for routing and name resolution.
- Web server(s) in the selected URLs reference.

File(s) to download from the machine I'm using to connect to the server

To download files from your machine to the server:

1. From the Download Files page, click **Browse** or enter the path to the file that resides on your machine. Specify 1 to 4 files to download.

2. When finished, click **Download**. Or if you need a signed file, at the bottom of the Web page, select the option, ***Install this File on the Local Server***, and click **Download**.

Note:

This signed file must be a `.tar` file. For example, `/testfile-1-1.i386.rpm.tar`

File(s) to download from the LAN using URL

To download files from a web server to the Avaya media server:

1. Specify 1 to 4 files to download by Universal Resource Locator (URL) address.
2. Specify the complete URL. For example, `https://networktime.com/security/keys.install`
3. If a proxy server is required for an external web server (not on the corporate network), it must be entered in a `server:port` format.
   - Enter the proxy server's name (such as network.proxy) or IP address.
   - If the proxy server requires a port number, add a colon (:) followed by a port number. The default proxy port is 80.
4. When finished, click **Download**. Or if you need a signed file, at the bottom of the Web page, select the option, Install this File on the Local Server, and click **Download**.

Note:

The signed file must be a `.tar` file. For example, `testfile-1-1.i386.rpm.tar`

Install this file on the local server

Use the **Install this file on the local server** option to download when you are instructed. This option allows you to download and install signed files. The file MUST be signed. Follow Avaya instructions to obtain your signed file. If you do not select the option, the files are retained in /var/home/ftp/pub and are not installed and signatures are not verified. However, files used for server upgrade could be downloaded without verifying the signatures.

Appendix A: Licenses

This section lists and provides examples of the licenses required by SES software and hardware.

Major applications

Each of the major software components has its own license, which are included below.

Table 8: Software and licenses

Software	License
Ace	ACE License
Apache	Apache License
Hughes SDF	Not open source—licensed from Hughes
Ismo	LGPL
Pear	Individual Licenses—see next table
Perl	ARtistic License
PHP	PHP license 3.0—attached
Postgres	Berkeley License
Red Hat 8	Red Hat License
Smarty	LGPL
Xerces	Apache License

PEAR Packages

PEAR packages are individually licensed by their contributors. These are summarized below.

Table 9: Pear software and licenses

Pear Software	License
PEAR core packages	2.02/4.02 PHP License
Config	2.02 PHP License
Validate	2.02 PHP License
XML/Tree	2.02 PHP License
Crypt/Xtea	2.02 PHP License
PHP	3.0
Net/URL	shown below
Log	none

PHP 3.0 License

```
--------------------------------------------------------------------
                  The PHP License, version 3.0
Copyright (c) 1999 - 2002 The PHP Group. All rights reserved.
--------------------------------------------------------------------

Redistribution and use in source and binary forms, with or without
modification, is permitted provided that the following conditions
are met:

  1. Redistributions of source code must retain the above copyright
     notice, this list of conditions and the following disclaimer.

  2. Redistributions in binary form must reproduce the above copyright
     notice, this list of conditions and the following disclaimer in
     the documentation and/or other materials provided with the
     distribution.

  3. The name "PHP" must not be used to endorse or promote products
     derived from this software without prior written permission. For
     written permission, please contact group@php.net.

  4. Products derived from this software may not be called "PHP", nor
     may "PHP" appear in their name, without prior written permission
     from group@php.net. You may indicate that your software works in
```

```
     conjunction with PHP by saying "Foo for PHP" instead of calling
     it "PHP Foo" or "phpfoo"

  5. The PHP Group may publish revised and/or new versions of the
     license from time to time. Each version will be given a
     distinguishing version number.
     Once covered code has been published under a particular version
     of the license, you may always continue to use it under the terms
     of that version. You may also choose to use such covered code
     under the terms of any subsequent version of the license
     published by the PHP Group. No one other than the PHP Group has
     the right to modify the terms applicable to covered code created
     under this License.

  6. Redistributions of any form whatsoever must retain the following
     acknowledgment:
     "This product includes PHP, freely available from
     <http://www.php.net/>".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM ``AS IS'' AND
ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP
DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT,
INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
OF THE POSSIBILITY OF SUCH DAMAGE.

--------------------------------------------------------------------

This software consists of voluntary contributions made by many
individuals on behalf of the PHP Group.

The PHP Group can be contacted via Email at group@php.net.

For more information on the PHP Group and the PHP project,
please see <http://www.php.net>.

This product includes the Zend Engine, freely available at
<http://www.zend.com>.
```

PHP 2.02/4.02 License

```
--------------------------------------------------------------------
                  The PHP License, version 2.02 4.02
Copyright (c) 1999 - 2002 The PHP Group. All rights reserved.
--------------------------------------------------------------------

Redistribution and use in source and binary forms, with or without
modification, is permitted provided that the following conditions
are met:

  1. Redistributions of source code must retain the above copyright
     notice, this list of conditions and the following disclaimer.

  2. Redistributions in binary form must reproduce the above
     copyright notice, this list of conditions and the following
     disclaimer in the documentation and/or other materials provided
     with the distribution.

  3. The name "PHP" must not be used to endorse or promote products
     derived from this software without prior permission from the
     PHP Group. This does not apply to add-on libraries or tools
     that work in conjunction with PHP. In such a case the PHP
     name may be used to indicate that the product supports PHP.

  4. The PHP Group may publish revised and/or new versions of the
     license from time to time. Each version will be given a
     distinguishing version number.

     Once covered code has been published under a particular version
     of the license, you may always continue to use it under the
     terms of that version. You may also choose to use such covered
     code under the terms of any subsequent version of the license
     published by the PHP Group. No one other than the PHP Group has
     the right to modify the terms applicable to covered code created
     under this License.

  5. Redistributions of any form whatsoever must retain the following
     acknowledgment:
     "This product includes PHP, freely available from
     http://www.php.net/".

  6. The software incorporates the Zend Engine, a product of Zend
     Technologies, Ltd. ("Zend"). The Zend Engine is licensed to the
     PHP Association (pursuant to a grant from Zend that can be
     found at http://www.php.net/license/ZendGrant/) for
     distribution to you under this license agreement, only as a
     part of PHP. In the event that you separate the Zend Engine
     (or any portion thereof) from the rest of the software, or
     modify the Zend Engine, or any portion thereof, your use of the
     separated or modified Zend Engine software shall not be governed
     by this license, and instead shall be governed by the license
     set forth at http://www.zend.com/license/ZendLicense/.
```

```
THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM ``AS IS'' AND
ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP
DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT,
INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
OF THE POSSIBILITY OF SUCH DAMAGE.

--------------------------------------------------------------------

This software consists of voluntary contributions made by many
individuals on behalf of the PHP Group.

The PHP Group can be contacted via Email at group@php.net.

For more information on the PHP Group and the PHP project,
please see <http://www.php.net>.
```

Perl – Artistic License

Preamble

The intent of this document is to state the conditions under which a Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over the development of the package, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

Definitions

“Package” refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.

“Standard Version” refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder as specified below.

“Copyright Holder” is whoever is named in the copyright or copyrights for the package.

“You” is you, if you're thinking about copying or distributing this Package.

"Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)

"Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.

You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:

- place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as uunet.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.
- use the modified Package only within your corporation or organization.
- rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.
- make other distribution arrangements with the Copyright Holder.

You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:

- distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.
- accompany the distribution with the machine-readable source of the Package with your modifications.
- give non-standard executables non-standard names, and clearly document the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.
- make other distribution arrangements with the Copyright Holder.

You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you do not advertise this Package as a product of your own. You may embed this Package's interpreter within an executable of yours (by linking); this shall be construed as a mere form of aggregation, provided that the complete Standard Version of the interpreter is so embedded.

The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whomever generated them, and may be sold commercially, and may be aggregated with this Package. If such scripts or library files are aggregated with this Package via the so-called "undump" or "unexec" methods of producing a binary executable image, then distribution of such an image shall neither be construed as a distribution of this Package nor shall it fall under the restrictions of Paragraphs 3 and 4, provided that you do not represent such an executable image as a Standard Version of this Package.

C subroutines (or comparably compiled subroutines in other languages) supplied by you and linked into this Package in order to emulate subroutines and variables of the language defined by this Package shall not be considered part of this Package, but are the equivalent of input as in Paragraph 6, provided these subroutines do not change the language in any way that would cause it to fail the regression tests for the language.

Aggregation of this Package with a commercial distribution is always permitted provided that the use of this Package is embedded; that is, when no overt attempt is made to make this Package's interfaces visible to the end user of the commercial distribution. Such use shall not be construed as a distribution of this Package.

The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The End

LGPL License

```
          GNU LESSER GENERAL PUBLIC LICENSE
               Version 2.1, February 1999

 Copyright (C) 1991, 1999 Free Software Foundation, Inc.
     59 Temple Place, Suite 330, Boston, MA  02111-1307  USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
 as the successor of the GNU Library Public License, version 2, hence
 the version number 2.1.]
```

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the

ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License").

Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses

the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a

medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding

machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library

facilities. This must be distributed under the terms of the
Sections above.

b) Give prominent notice with the combined library of the fact
that part of it is a work based on the Library, and explaining
where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed

through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE

LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING
RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A
FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF
SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH
DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

> <one line to give the library's name and a brief idea of what it does.>
> Copyright (C) <year> <name of author>
>
> This library is free software; you can redistribute it and/or
> modify it under the terms of the GNU Lesser General Public
> License as published by the Free Software Foundation; either
> version 2.1 of the License, or (at your option) any later version.
>
> This library is distributed in the hope that it will be useful,
> but WITHOUT ANY WARRANTY; without even the implied warranty of
> MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
> Lesser General Public License for more details.
>
> You should have received a copy of the GNU Lesser General Public
> License along with this library; if not, write to the Free Software
> Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

> Yoyodyne, Inc., hereby disclaims all copyright interest in the
> library `Frob' (a library for tweaking knobs) written by James Random Hacker.
>
> <signature of Ty Coon>, 1 April 1990
> Ty Coon, President of Vice

That's all there is to it!

PHP Net/URL License

```
// +----------------------------------------------------------------------+
// | Copyright (c) 2002-2003, Richard Heyes                               |
// | All rights reserved.                                                 |
// |                                                                      |
// | Redistribution and use in source and binary forms, with or without   |
// | modification, are permitted provided that the following conditions   |
// | are met:                                                             |
// |                                                                      |
// | o Redistributions of source code must retain the above copyright     |
// |   notice, this list of conditions and the following disclaimer.|
// | o Redistributions in binary form must reproduce the above copyright  |
// |   notice, this list of conditions and the following disclaimer in the |
// |   documentation and/or other materials provided with the distribution.|
// | o The names of the authors may not be used to endorse or promote     |
// |   products derived from this software without specific prior written  |
// |   permission.|
// |                                                                      |
// | THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS  |
// | "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT    |
// | LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR |
// | A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT  |
// | OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, |
// | SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT     |
// | LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, |
// | DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY |
// | THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT  |
// | (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE |
// | OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. |
// |                                                                      |
// +----------------------------------------------------------------------+
// | Author: Richard Heyes <richard@php.net>                              |
// +----------------------------------------------------------------------+
```

Postgresql License

```
Legal Notice
  PostgreSQL is Copyright © 1996-2001
  by the PostgreSQL Global Development Group and is distributed under
  the terms of the license of the University of California below.

  Postgres95 is Copyright © 1994-5
  by the Regents of the University of California.

  Permission to use, copy, modify, and distribute this software and
  its documentation for any purpose, without fee, and without a
  written agreement is hereby granted, provided that the above
  copyright notice and this paragraph and the following two paragraphs
  appear in all copies.
```

```
IN NO EVENT SHALL THE UNIVERSITY OF CALIFORNIA BE LIABLE TO ANY
PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL
DAMAGES, INCLUDING LOST PROFITS, ARISING OUT OF THE USE OF THIS
SOFTWARE AND ITS DOCUMENTATION, EVEN IF THE UNIVERSITY OF CALIFORNIA
HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE UNIVERSITY OF CALIFORNIA SPECIFICALLY DISCLAIMS ANY WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE
PROVIDED HEREUNDER IS ON AN "AS-IS" BASIS, AND THE UNIVERSITY OF
CALIFORNIA HAS NO OBLIGATIONS TO PROVIDE MAINTENANCE, SUPPORT,
UPDATES, ENHANCEMENTS, OR MODIFICATIONS.
```

Apache License

```
/* ====================================================================
 * The Apache Software License, Version 1.1
 *
 * Copyright (c) 2000 The Apache Software Foundation. All rights
 * reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. The end-user documentation included with the redistribution,
 *    if any, must include the following acknowledgment:
 *       "This product includes software developed by the
 *        Apache Software Foundation (http://www.apache.org/)."
 *    Alternately, this acknowledgment may appear in the software itself,
 *    if and wherever such third-party acknowledgments normally appear.
 *
 * 4. The names "Apache" and "Apache Software Foundation" must
 *    not be used to endorse or promote products derived from this
 *    software without prior written permission. For written
 *    permission, please contact apache@apache.org.
 *
 * 5. Products derived from this software may not be called "Apache",
 *    nor may "Apache" appear in their name, without prior written
 *    permission of the Apache Software Foundation.
 *
 * THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED
 * WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
```

```
* OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
* DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
* LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
* USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND
* ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
* OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT
* OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
* ====================================================================
*
* This software consists of voluntary contributions made by many
* individuals on behalf of the Apache Software Foundation. For more
* information on the Apache Software Foundation, please see
* <http://www.apache.org/>.
*
* Portions of this software are based upon public domain software
* originally written at the National Center for Supercomputing Applications,
* University of Illinois, Urbana-Champaign.
*/
```

Red Hat 8 License

LICENSE AGREEMENT AND LIMITED PRODUCT WARRANTY

RED HAT LINUX 8.0 PROFESSIONAL EDITION

Please read this document carefully before installing Red Hat® Linux®, any of its packages, or any software included with this product, on your computer. This document contains important information about your legal rights. By installing any or all of the software included with this product, you agree to the following terms and conditions.

GENERAL

As used herein, “EULA” means an end user license agreement, and “Software Programs” means, collectively, the Linux Programs and the Third-Party Programs, as each of those terms is defined herein.

Red Hat Linux is a modular operating system made up of hundreds of individual software components, each of which was individually written and copyrighted. Throughout this document these components are referred to, individually and collectively, as the "Linux Programs." Each Linux Program has its own applicable end user license agreement. Most of the Linux Programs are licensed pursuant to an open source EULA that permits you to copy, modify, and redistribute the software, in both source code and binary code forms. With the exception of the content of certain image files identified below, the remaining Linux Programs are freeware or have been placed in the public domain. To understand the applicable EULA for each Linux Program, your rights under it and to realize the maximum benefits available to you with Red Hat Linux, you must review the on-line documentation that accompanies each Linux Program. Nothing in this license agreement limits your rights under, or grants you rights that supersede, the terms of any applicable EULA.

The "Office and Multimedia Applications CD" includes an assortment of applications from third-party vendors. Throughout this document each of these software components are referred to, individually and collectively, as "Third-Party Programs." Generally, each of these Third-Party Programs is licensed to you by the vendor pursuant to an end user license agreement ("Third-Party EULA") that generally permits you to install each of these products on only a single computer for your own individual use. Copying, redistribution, reverse engineering, and/or modification of these components may be prohibited, and you must look to the terms and conditions of the Third-Party EULA to determine your rights and any limitations imposed on you. Any violation by you of the applicable Third-Party EULA terms shall immediately terminate your license under that Third-Party EULA. For the precise terms of the Third-Party EULAs for each of these Third-Party Programs, please check the on-line documentation that accompanies each of them. If you do not agree to abide by the applicable license terms for these Third-Party Programs, then do not install them on your computer.

If you wish to install any of these Third-Party Programs on more than one computer, please contact the vendor of the Third-Party Program to purchase additional licenses.

Red Hat Linux itself is a collective work under U.S. copyright law. Subject to the trademark use limitations set forth in this Agreement, Red Hat grants you a license in the collective work pursuant to the GNU General Public License.

BEFORE INSTALLATION

CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE INSTALLING ANY OF THE SOFTWARE PROGRAMS. INSTALLING THE SOFTWARE PROGRAMS INDICATES YOUR ACCEPTANCE TO THE TERMS AND CONDITIONS SET FORTH IN THIS DOCUMENT AND OF THE END USER LICENSE AGREEMENT ASSOCIATED WITH THE SOFTWARE PROGRAM. IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, DO NOT INSTALL THE SOFTWARE PROGRAMS.

THE SOFTWARE PROGRAMS, INCLUDING SOURCE CODE, DOCUMENTATION, APPEARANCE, STRUCTURE AND ORGANIZATION, ARE PROPRIETARY PRODUCTS OF RED HAT, INC. AND OTHERS AND ARE PROTECTED BY COPYRIGHT AND OTHER LAWS. TITLE TO THESE PROGRAMS, OR TO ANY COPY, MODIFICATION OR MERGED PORTION OF ANY OF THESE PROGRAMS, SHALL AT ALL TIMES REMAIN WITH THE AFOREMENTIONED, SUBJECT TO THE TERMS AND CONDITIONS OF THE APPLICABLE EULA RELATED TO THE SOFTWARE PROGRAMS UNDER CONSIDERATION.

THE “RED HAT” TRADEMARK, THE "BLUECURVE" TRADEMARK AND RED HAT'S SHADOW MAN LOGO ARE REGISTERED TRADEMARKS OF RED HAT, INC. IN THE UNITED STATES AND OTHER COUNTRIES. WHILE THIS LICENSE AGREEMENT ALLOWS YOU TO COPY, MODIFY AND DISTRIBUTE THE SOFTWARE, IT DOES NOT PERMIT YOU TO DISTRIBUTE THE SOFTWARE UTILIZING RED HAT'S TRADEMARKS. YOU SHOULD READ THE INFORMATION FOUND AT http://www.redhat.com/about/trademark_guidelines.html

BEFORE DISTRIBUTING A COPY OF THE SOFTWARE, REGARDLESS OF WHETHER IT HAS BEEN MODIFIED. IN ADDITION, IF YOU MAKE A COMMERCIAL REDISTRIBUTION OF THE SOFTWARE AND (A) YOU DO NOT FALL WITHIN AN EXCEPTION PROVIDED IN RED

HAT'S TRADEMARK GUIDELINES, (B) YOU HAVE NOT ENTERED INTO A REDISTRIBUTION AGREEMENT WITH RED HAT, OR (C) YOU DO NOT HAVE A TRADEMARK LICENSE AGREEMENT WITH RED HAT, THEN YOU MUST MODIFY THE FILES IDENTIFIED AS REDHAT-LOGOS AND ANACONDA-IMAGES SO AS TO REMOVE ALL USE OF IMAGES CONTAINING THE "RED HAT" TRADEMARK OR RED HAT'S SHADOW MAN LOGO. NOTE THAT MERE DELETION OF THOSE FILES MAY CORRUPT THE SOFTWARE.

CERTAIN LIMITED TECHNICAL SUPPORT SERVICES ACCOMPANY RED HAT LINUX. THE RIGHT TO USE THOSE TECHNICAL SUPPORT SERVICES ARE LIMITED TO THE ORIGINAL PURCHASER OF THE PRODUCT FROM EITHER RED HAT OR A RED HAT AUTHORIZED DISTRIBUTOR. WHILE YOU HAVE THE RIGHT TO TRANSFER YOUR COPY OF RED HAT LINUX TO ANOTHER PARTY, YOU MAY NOT TRANSFER THE RIGHT TO USE THOSE TECHNICAL SUPPORT SERVICES ONCE YOU HAVE ACTIVATED YOUR PRODUCT FOR SUPPORT. ANY ATTEMPT TO TRANSFER TECHNICAL SUPPORT SERVICES FOLLOWING ACTIVATION WILL RENDER YOUR RIGHT TO THE TECHNICAL SUPPORT SERVICES NULL AND VOID.

LIMITED WARRANTY

EXCEPT AS SPECIFICALLY STATED IN THIS AGREEMENT OR IN AN EULA, THE SOFTWARE PROGRAMS ARE PROVIDED AND LICENSED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Red Hat, Inc. warrants that the media on which any of the Software Programs are furnished will be free from defects in materials and manufacture under normal use for a period of 30 days from the date of delivery to you. Red Hat, Inc. does not warrant that the functions contained in the Software Programs will meet your requirements or that the operation of the Software Programs will be entirely error free or appear precisely as described in the accompanying documentation.

ANY WARRANTY OR REMEDY PROVIDED UNDER THIS AGREEMENT EXTENDS ONLY TO THE PARTY WHO PURCHASES RED HAT LINUX FROM RED HAT OR A RED HAT AUTHORIZED DISTRIBUTOR.

LIMITATION OF REMEDIES AND LIABILITY

To the maximum extent permitted by applicable law, the remedies described below are accepted by you as your only remedies, and shall be available to you only if you or your dealer registers this product with Red Hat, Inc. in accordance with the instructions provided with this product within ten days after delivery of the Software Programs to you.

Red Hat, Inc.'s entire liability, and your exclusive remedies, shall be: if the Software Programs media are defective, you may return them within 30 days of delivery to you along with a copy of your receipt and Red Hat, Inc., at its option, will replace them or refund the money paid by you for the Software Programs. **TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL RED HAT, INC. BE LIABLE TO YOU FOR ANY DAMAGES, INCLUDING LOST PROFITS, LOST SAVINGS, OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES, ARISING OUT OF THE USE OR INABILITY TO USE THE**

SOFTWARE PROGRAMS, EVEN IF RED HAT, INC. OR A DEALER AUTHORIZED BY RED HAT, INC. HAD BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

GENERAL

If any provision of this Agreement is held to be unenforceable, that shall not effect the enforceability of the remaining provisions. This Agreement shall be governed by the laws of the State of North Carolina and of the United States, without regard to any conflict of laws provisions.

ACE License

Copyright and Licensing Information for ACE™ and TAO™

ACE™ and TAO™ are copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University Copyright (c) 1993-2003, all rights reserved. Since ACE+TAO are open-source, free software, you are free to use, modify, copy, and distribute--perpetually and irrevocably--the ACE+TAO source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using ACE+TAO.

You can use ACE+TAO in proprietary software and are under no obligation to redistribute any of your source code that is built using ACE+TAO. Note, however, that you may not do anything to the ACE+TAO code, such as copyrighting it yourself or claiming authorship of the ACE+TAO code, that will prevent ACE+TAO from being distributed freely using an open-source development model. You needn't inform anyone that you're using ACE+TAO in your software, though we encourage you to let us know so we can promote your project in the ACE+TAO success stories.

ACE+TAO are provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, non-infringement, or arising from a course of dealing, usage or trade practice. Moreover, ACE+TAO are provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. However, commercial support for ACE is available from Riverace and commercial support for TAO is available from OCI and PrismTech. Both ACE and TAO are Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by ACE+TAO or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE and TAO web sites are maintained by the Center for Distributed Object Computing of Washington University for the development of open-source software as part of the open-source software community. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the ACE and TAO software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source ACE+TAO projects or their designees.

The names ACE™, TAO™, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE™ or TAO™, nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

Appendix B: Worksheet for Duplication

Contents of this appendix

This section provides a work sheet to help with names and prompt responses for installation and configuration. This work sheet is for duplexed, separated home and edge servers.

Edge-A is the primary edge server.

Edge-B is the duplexed backup server of A.

Home1A is the primary home server.

Home1B is the backup server.

Home 2 is installed as simplex

ccsInstaller

Start with edge servers, duplex configuration for failover.

primary edge server

Edge-A	Example response
Host Name	ccsedgeA
DNS Domain Name:	avayaSIP.com
IP Address:	176.21.20.176
Netmask:	255.255.254.0
Gateway:	176.21.21.254
Primary DNS IP Address:	192.168.1.21
Secondary DNS IP Address:	none
Tertiary DNS IP Address:	none
Host name of RMB card	ccsedgeA-rmb
IP Address of RMB eth port:	default
Netmask of RMB eth port:	default
Gateway of RMB eth port:	default
Install High Availability Option?	Y
My role in redundant infrastructure?	A
Logical name of Redundant system:	ccsedge
Logical IP Address of Redundant system:	176.21.20.205
Host Name of [B] Server	ccsedgeB
IP Address of [B] Server	176.21.20.177
User Name of A server RMB Login	craft
Enter Password of [A] Server RMB Login USERID	See Maestro
Password Repeat	

Edge-A	Example response
Hostname of [B] Server RMB Card:	ccsedgeB-rmb
User name of [B] Server RMB Login:	craft
Enter password of [B] Server RMB Login:	See Maestro
Password Repeat	
Abort waiting and make this one primary?	DO NOT ANSWER
Init a Master Administrator? (asked only on First Server)	Y
mvss db password	See Maestro
password repeat	
DB INITIALIZES...WAIT	
Start services?	NO!
SEE DOCUMENTATION BEFORE STARTING SERVICES	

backup edge server

Edge-B	Example response
Host Name:	ccsedgeB
Domain Name:	avayaSIP.com
IP Address:	176.21.20.177
Netmask:	255.255.254.0
Gateway:	176.21.21.254
primary DNS IP Address:	192.168.1.21
Secondary DNS IP Address:	none
Tertiary DNS IP Address	none
Host name of RMB card:	ccsedgeB-rmb
IP Address of RMB eth port:	default
Netmask of RMB eth port:	default
Gateway of RMB eth port:	default
Install High Availability Option?	Y
My role in redundant infrastructure?	B (default)
Logical name of Redundant system:	ccsedge
Logical IP Address of Redundant system:	176.21.20.205
Host Name of [B] Server	ccsedggea
IP Address of [B] Server	176.21.20.176
User Name of A server RMB Login	craft
Enter Password of [A] Server RMB Login USERID	See Maestro
Password Repeat	

Edge-B	Example response
Hostname of [B] Server RMB Card:	ccsedgeB-rmb
User name of [B] Server RMB Login:	craft
Enter password of [B] Server RMB Login:	See Maestro
Password Repeat	
Abort waiting and make this one primary?	DO NOT ANSWER
mvss db password	See Maestro
password repeat	
DB INITIALIZES...WAIT	
Start services?	NO!
SEE DOCUMENTATION BEFORE STARTING SERVICES	

primary home server

Home1-A	Example response
Host Name:	ccshome1A
SIP Domain Name:	avayaSIP.com
IP Address:	176.21.20.178
Netmask:	255.255.254.0
Gateway:	176.21.21.254
primary DNS IP Address:	192.168.1.21
Secondary DNS IP Address:	none
Tertiary DNS IP Address:	none
Host name of RMB card:	ccshome1A-rmb
IP Address of RMB eth port:	default
Netmask of RMB eth port:	default
Gateway of RMB eth port:	default
Install High Availability Option?	Y
My role in redundant infrastructure?	A
Logical name of Redundant system:	ccshome
Logical IP Address of Redundant system:	172.21.20.200
Host Name of [B] Server	ccshome1B
IP Address of [B] Server	172.21.20.179
User Name of A server RMB Login	craft
Enter Password of [A] Server RMB Login USERID	See Maestro
Password Repeat	

Home1-A	Example response
Hostname of [B] Server RMB Card:	ccshome1B-rmb
User name of [B] Server RMB Login:	craft
Enter password of [B] Server RMB Login:	See Maestro
Password Repeat	
Abort waiting and make this one primary?	DO NOT ANSWER
Init a Master Administrator? (asked only on First Server)	N
mvss db password	mvss See Maestro
password repeat	
DB INITIALIZES...WAIT	
Start services?	NO!
SEE DOCUMENTATION BEFORE STARTING SERVICES	

backup home server

Home1-B	Example response
Host Name:	ccshome1B
Domain Name:	avayaSIP.com
IP Address:	172.21.20.179
Netmask:	255.255.254.0
Gateway:	172.21.21.254
primary DNS IP Address:	192.168.1.21
Secondary DNS IP Address:	none
Tertiary DNS IP Address:	none
Host name of RMB card:	ccshome1B-rmb
IP Address of RMB eth port:	default
Netmask of RMB eth port:	default
Gateway of RMB eth port:	default
Install High Availability Option?	Y
My role in redundant infrastructure?	B
Logical name of Redundant system:	ccshome
Logical IP Address of Redundant system:	172.21.21.206
Host Name of [B] Server	ccshome1A
IP Address of [B] Server	172.21.20.178
User Name of A server RMB Login	craft
Enter Password of [A] Server RMB Login USERID	See Maestro
Password Repeat	

Home1-B	Example response
Hostname of [B] Server RMB Card:	ccshome1A-rmb
User name of [B] Server RMB Login:	craft
Enter password of [B] Server RMB Login:	See Maestro
Password Repeat	
Abort waiting and make this one primary?	DO NOT ANSWER
mvss db password	See Maestro
password repeat	
DB INITIALIZES...WAIT	
Start services?	NO!
SEE DOCUMENTATION BEFORE STARTING SERVICES	

Appendix C: Force All and Update All use and behavior

This section compares and contrasts the Force All command and the Update command. Find the following topics in this discussion.

Function and Purpose

This section explains what these two commands are for, and how they are meant to be used.

Function and Purpose of the Update All Command	Function and Purpose of the Force All command
The **Update All** command is the default mechanism for distributing data between the Master Administration system and the SES home server, where most run-time operations occur, as well as the edge server. **Update All** tracks the changes made during administration, and then when executed, copies those changes down to the SES servers.	The **Force All** command is similar to Update All in that it copies data from the Master Administration system to the run-time databases of the SES home and edge servers. Its need is indicated by the highlighted update button in the menu on the left.
Only the data modified since the last update is copied, making the Update All function light weight and efficient. There is no limitation on using the Update All function, and no noticeable impact on the run-time system. Use Update All whenever changes are made to the master administration database. Its need is indicated by the highlighted Update button in the menu on the left. Its need is indicated by the highlighted update button in the menu on the left.	However, instead of being an incremental update, **Force All** removes all the data on the run-time server and does a blind copy of all the data from the Master Admin system. This operation can be very time consuming and CPU intensive for medium to large systems.The time required to complete a Force All is completely dependent on system configuration. The time to complete the Force All increases as more home servers and users are added to the configuration.
If the home server's databases are out of sync with the Master Administration system database, select the **Force All** menu item on the edge server or home/edge server to synchronize all hosts. This situation may occur after a failed **Update All**.	

Function and Purpose of the Update All Command (continued)	Function and Purpose of the Force All command (continued)
Not executing **Update All** results in user data, edge data, and media server data not being pushed to the home servers. This non-synchronization ultimately causes many problems. Users cannot log in, and make calls, due to the run-time database not containing the data they require.	In a **Force All** and a **Force Node**, the edge server is always updated first. Home servers are updated in alphabetical order by hostname. Even if a **Force Node** is executed for a home server, the edge is updated first, followed by the selected home server. For a **Force All**, once the edge server is completed, the home servers are updated in alphabetical order by host name.
If a database error is seen during an **Update All**, and the update does not complete, you should execute a **Force All** or **Force** command for the individual node to where the changes are directed.	Command logging for the **Force All** and **Update All** commands are kept in `/var/log/sip-server/ImpressLog.txt`. The log contains a message and timestamp for when each of the commands was started and completed. The log contains a message and timestamp for when **Force All** was started and completed. This log is kept in /var/log/sip-server/ImpressLog.txt. **Force** executes a **Force All** for an individual node. Force completely wipes out the mvss database on the selected SES server and reconstruct its data from the data contained in the mvss_admin database on the edge or master administration subsystem.

When to use

This section explains when to use Update All and when to use Force all.

When to use Update All	When to use Force All
Use **Update All** whenever changes are made to the Master Administrations system's database. A need for **Update All** is indicated by the highlighted update button in the menu on the left.	The use of **Force All** should be limited and only done under the following circumstances:
The *only* time you should ignore the highlighted **Update** button is following a Migrate Home/Edge. After executing a Migrate Home/Edge, the **Update** button is highlighted, and you should press the Continue button, on the Confirm Migrate Home/Edge page, to invoke an automatic **Force All** or execute **Force All** from the **List Hosts** screen. See notes on **Force All**.	• An import of a ProVision XML file. Once the file is successfully imported, pressing Continue automatically invokes a **Force All**. Pressing Continue to invoke the **Force All** is required and MUST be done for proper server operation.
	• Following a Migrate Home/Edge to an edge with a home. Once the system has been successfully migrated, pressing Continue automatically invokes a **Force All**. Pressing Continue to invoke the **Force All** is required and MUST be done for proper server operation.
Several changes may be made to the Master Admin system before the Update or **Update All** button is pressed. There is no need to hit Update after every single change. The changes are batched using **Update All**.	
However, if many changes are being made to master admin, it is good practice to hit Update after several changes rather than waiting for all changes to be made, then hitting Update.	• The IP address of a server has changed, usually with the Edit Host screen. If the IP address of a server is changed, the system displays a message indicating that a **Force All** must be done and to press OK to invoke the automatic **Force All**.
Update All is the routine mechanism to push data to the home servers. You do not need to limit its use.	
If an error is seen during an **Update All**, this indicates data inconsistency and a **Force All** or individual force should be executed to rectify the databases.	• A database error is seen during an **Update All**. A database error seen during an **Update All** can usually be cleared by doing a Force for the home server from the List Host page, or by doing a **Force All**.

When to use Update All (continued)	When to use Force All (continued)
	• If an individual Force for a home fails, execute a **Force All**. • After an upgrade, if things do not appear to be working correctly, execute a **Force All**. Following a software upgrade, a **Force All** should not have to be done. However, if things do not appear to be working properly, a **Force All** should be executed. Select **Hosts** from the menu to use **Force All** only when you believe that user or system data are out of sync between the edge and home servers. This can occur if a previously executed **Update All** failed. When an SES server is out of service, perhaps for maintenance, select **Force All** to synchronize the databases on all hosts. This choice may cause a temporary outage of service.

Effects on SIP Service

This section explains what happens to your SIP service when you use these commands.

SIP Service Effects of Update All	SIP Service Effects of Force All
There should be minimal to no effect on SIP transactions during an update all. Postgres will only update those users or entities that were changed.	During a **Force All**, Postgres progressively locks the record being updated, making it read-only. Service to end uses should only be affected if a user is trying to make a changes during the postgres update. the updates are done sequentially, so as the **Force All** progresses, data that have been updated is unlocked by postgres. However, due to the huge task force all is executing, CPU occupancy will be higher during that time and may affect the peak performance rates during that period and may adversely affect call completion. **Force All** completely wipes out the mvss database on all SES servers and reconstructs them from the data contained in the mvss_admin database on the edge, or master administration system. The time required to complete a **Force All** is completely dependent on system configuration. The time required increases with the number of home servers and users. In small systems, this may be a matter of minutes. Larger systems may take an hour to several hours to complete a **Force All**.

Effects on Service

This section explains what happens to overall SIP service when you use these commands.

Service Effects of Update All	Service Effects Force All
There should be minimal to no effect on PPM transactions during an update all. Postgres only updates those users or entities that were changed.	Same as the effect on SIP transactions. As soon as the data are updated for a given user, that user is able to resume changing data. During the update of an individual record, only read-only operations return successful.

Appendix D: SNMP Alerts

What is in this appendix

Read about the SES R3.0 SNMP alerts presented in these sections:

- Be sure to read this on page 479, explanation of event numbering
- Managing traps on page 479
- Events on page 481 described
- MIB object ID on page 510 described

To find SNMP traps by name and not object ID, see the Index of SNMP traps on page 511. Click on the page number there to jump to a trap description.

Be sure to read this

If you are new to MIB or SNMP, this section may prevent misunderstanding and save you time.

- Notice when you read the tables that `sysUpTime` and `sysObjectID` are imported from MIB-II.
- Each group of alerts uses a different object ID for the base, and then appends the object ID (OID) shown in the table.
- In the first table in CPU monitor trap on page 482, append the OID shown in the table, for instance **.3**, to 1.3.6.1.4.1.6889.2.5.1.**1** to obtain the full object ID, which is 1.3.6.1.4.1.6889.2.5.**1**.**3**.

Managing traps

SNMP enables the SIP Enablement Services system to do the following things:

- Report the alarm events to the external manager entities such as Avaya INADS, Avaya Fault Performance Manager, Avaya Network Management System, and third party entities (for example, HP OpenView).
- Respond to the query requests from the external manager entities for the product configuration information.

Network management using SNMP requires several components:

- Network manager or management station such as FPM or HP OpenView
- Managed network element's agent
- Management information base (MIB)

The customer supplies the network management station. The agent and MIBs are typically supplied by the network element vendor. The agent is co-resident with the managed element and is a subcomponent of the platform management system. MIBs are either standard or custom-built from the vendor. SIP Enablement Services supports certain groups of the IETF standard MIB-II as well as a custom Avaya CCS MIB.

Remote maintenance boards

The SES hardware platform supports two types of remote maintenance boards (RMB):

- Remote Supervisor Adaptor or RSA
- Server Availability Management Processor or SAMP

The ethernet port of the these RMBs enables the IP-based services, including the SNMP traps and SNMP Query of S8500 server. The RMB acts as its own SNMP entity, independently of the SES system.

This extra reporting mechanism is extremely helpful. If SES processes or the SES server itself is down, it cannot report its own condition. The RMB provides the capability to restart and monitor processes on the SES server.

Remote Supervisor Adaptor

The S8500 server uses a PCI plug-in remote maintenance board called Remote Supervisor Adaptor (RSA). The RSA on the S8500s are a self-sufficient maintenance entity to monitor the operation of a S8500 platform. RSA has a built-in SNMP Agent and its own web-based configuration pages.

The RSA card has a serial port and two ethernet ports that allow access to the SES hardware and reporting to network management entities.

Server Availability Management Processor

The series S8500 hardware platform has a similar component to the RSA called the Server Availability Management Processor. In an S8500B, the remote maintenance board is a SAMP.

The SAMP remote maintenance board in the series S8500 hardware platform does not support SNMP traps.

Events

This section discusses SNMP events into these sections:

- Trap definitions
- Standard MIB support
- Traps resulting in INADS call

In the tables in all these sections, **RO** indicates Read Only and **NA** means Not Applicable.

Traps with a severity of **warning** are sent as traps, but are logged in syslog and the alarm log only:

avCCSDBStart	avCCSProcessStart
avCCSEthfaultclear	avCCSRegRegAuthfailed (note the letter g)
avCCSEvtSrvCMSubRetry	avCCSRegReqAuthfailed (note the q)
avCCSEvtSrvCMResubscribe	avCCSSerialLinkUp
avCCSEvtSrvSubsRej	avCCSUPSstatus
avCCSProcessStop	avCCSVacuumOK

The exceptions are the following traps, which are not true traps but are defined as such in the MIB. These traps are logged in syslog, but *not* in the alarm log:

avCCSApacheStart	avCCSSerialLinkUp
avCCSDBStart	avCCSUpgradeOK
avCCSEthFaultClear	avCCSVacuumOK
avCCSProcessStart	

Trap definitions

The following traps are in the ccs-traps group.

Append the OID shown in the table to 1.3.6.1.4.1.6889.2.5.1.4 to obtain the full OID.

CPU monitor trap

The CPU monitor checks every 5 minutes for a duration of 1 minute. If the average CPU utilization is 80% or greater, this trap is sent.

The following trap, with supporting information, is generated by the CPU:

OID	Object Type	Description	Variables
.3	avCCSCPUutilization minor	CPU utilization is at least 80%	sysUpTime sysObjectID acCCSIPAddress acCCCSHostname avCCSalarmType avCCSproductID
CPU utilization is at least 80%. If this situation persists, contact Avaya Services.			

Ethernet links traps

Ethernet bus faults may result in complete loss of server functionality, possible the public link interfaces with clients and the private links for duplication purposes. The services link is not monitored.

The following traps are generated by the ethernet bus:

OID	Object Type	Description	Variables
.5	avCCSEthfaultPublic major	An ethernet link fault has occurred on the public interface.	sysUpTime, sysObjectID, avCCSIPAddress, avCCSHostname avCCSalarmType avCCSproductID
The SES server's *public* ethernet interface is no longer operational. Verify that there is physical connection to this port and that network connectivity exists on other hosts on the same network. If this situation persists, contact Avaya Services.			
.6	avCCSEthfaultPrivate major	An ethernet link fault has occurred on the private interface.	sysUpTime, sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSproductID
The SES server's *private* ethernet interface is no longer operational. Check the LAN cable and connection between the two servers. Verify the physical connection to this port and the connectivity on other hosts. If this situation persists, contact Avaya Services.			

OID	Object Type	Description	Variables
.7	avCCSEthfaultclear warning	The ethernet bus fault has been cleared	sysUpTime, sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSproductID
The ethernet fault previously identified is cleared now.			

Disk error traps

Disk errors are significant to the health of the SES system. The following traps reflect disk errors:

OID	Object Type	Description	Variables
.10	avCCSDiskWarning* major	The data disk is 90% full	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSDiskPartition
The data disk is 90% full. Take immediate action to avoid a service outage. Back up any logs, temp files, and any superfluous data to another disk. If this error is due to log file accumulation, delete old logs, with approval, or move big logs to off-line storage. Depending on which disk partition is filling, the remedy can be different. This is a administration issue and resolution may be specific for your installation.			
.11	avCCSNoDiskSpace** major	The data disk is 98% full.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSDiskPartition
The data disk is full. This error causes loss of service to if not corrected. Depending on which disk partition is filling, the remedy can be different. This is an administration issue and resolution may be specific for your installation.			

* Each disk partition is checked every 10 minutes. The database partition has a threshold of 60% full. Other partitions have a threshold of 90%. Once the threshold is crossed, the system sends the `ccsDiskWarning` error.

**For the `ccsNoDiskSpace` trap, the database partition has a threshold of 80% full. Other partitions have a threshold of 98%.

Watchdog event traps

Watchdog traps were formerly based on Watchdog events. Now, they reflect events of processes *monitored* by the Watchdog.

The following traps are generated by the Watchdog process about their watched events:

OID	Object Type	Description	Variables
.15	avCCSProcessStart warning	The watchdog-monitored process has started.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSProcess
.16	avCCSProcessStartFailed major	The watchdog-monitored process has failed to start.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSProcess
.17	avCCSProcessStop warning	The watchdog-monitored process has stopped.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSProcess

Critical server events traps

The following traps are generated by critical events occurring on a server:

OID	Object Type	Description	Variables
.18	avCCSVIPFault major	The Virtual IP address is not operational on this server.	sysUpTime, sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The virtual IP address used for server redundancy is no longer operational. This can happen if someone configures another server with the same IP address. Find the erroneous, duplicate IP addresses and change one of them.			
.19	avCCSRAID1 major	The RAID 1 system is not operational.	sysUpTime, sysObjectID, avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Contact Avaya Services.			
.20	avCCSMonfault major	A required system process has stopped responding to MON.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
A required system process has stopped responding to MON. From the Maintenance interface, view the Process Status screen to verify this. Reboot the server and verify that MON is running. If the situation persists, contact Avaya Services.			
.21	avCCSDRBDFault major	DRBD cannot be loaded or executed.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
DRBD (distributed redundant block device) cannot be loaded or executed. The system is no longer redundant. See the avCCSHAFault error prior to this one. Call Avaya Services immediately.			

OID	Object Type	Description	Variables
.22	avCCSIPfailFault critical	IPfail cannot be loaded or executed	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
IPfail cannot be loaded or executed. Reboot the server. If the situation persists, contact Avaya Services.			

Duplicate server events traps

The traps in this section apply only when your system's configuration is duplex, that is, has a backup server for either a home/edge, home, or edge server.

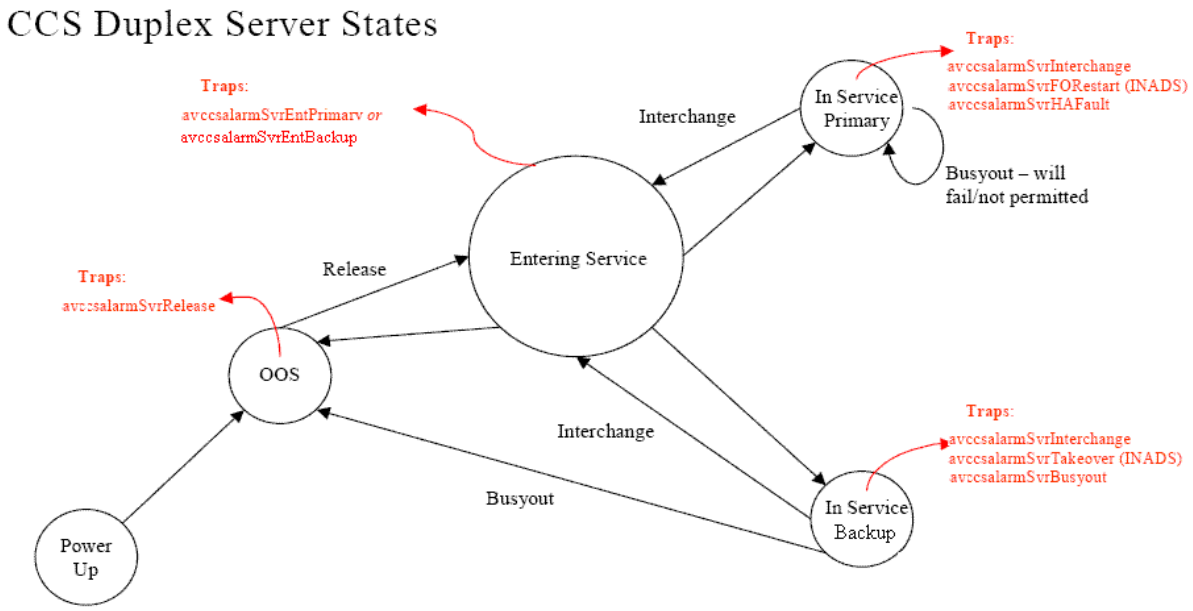
Figure 139 shows two important concepts:

- The direction and type of state changes that can occur for any server.
- The changes of state a duplex server may go through in the event of critical errors

A duplexed server *must* be aware of its duplicate status, primary or backup. All duplex traps are considered critical.

All administrative busyouts and releases are trapped and logged.

Figure 139: Duplex Server State Changes



OID	Object Type	Description	Variables
.23	avCCSHAfault major	The server is no longer redundant.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
A fault of the redundant pair has been detected. The high availability operation is down. To resolve this alarm: 1. Check the system status by viewing the Maintenance interface, Status Summary screen. 2. If the server has been busied out, then click the Release Server screen of Maintenance interface to put the server back to service 3. If the alarm persists, escalate the problem to Avaya Services. If this error is not corrected, you might see avCCSDRBDFault. Call Avaya Services immediately.			
.24	avCCSFORestart major	The system has failed over to the backup system	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID

OID	Object Type	Description	Variables
The backup server has restarted as the primary server due to the failover. The original primary server may experience non-recoverable faults. To resolve this alarm: 1. View the Status Summary screen to verify the status of redundant system which should be primary / backup 2. If not, escalate the problem to Avaya Services.			
.81	avCCSSrvBusyout minor	The server has been administratively busied out.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The server has been busied out manually. The redundant system cannot provide high availability operation. To resolve this alarm: 1. Check the system status by clicking Status Summary screen of the Maintenance interface. 2. If the server has been busied out, then click the Release Server screen of Maintenance interface to restore the server back to service. 3. If the alarm persists, escalate the problem to Avaya Services.			
.82	avCCSSrvRelease minor	The server has been administratively released.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The server has been manually released back to service. The redundant system is in transition to the high availability operation. To resolve this alarm: 1. Check the system status by clicking Status Summary screen of Maintenance interface. The Status Summary should show the state primary / backup 2. If the server is not in primary/ backup state, escalate the problem to Avaya Services.			
.83	avCCSSrvInterchange major	The server has been administratively interchanged.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID

OID	Object Type	Description	Variables
A system administrator has initiated an interchange using the Interchange Server screen of the Maintenance interface. 1. Check the system status by clicking Status Summary screen of Maintenance interface The Status Summary should show the state primary/ backup 2. If the server is not in primary/ backup state, escalate the problem to Avaya Services			
.84	avCCSSrvEntPrimary minor	The server is entering service as the primary server	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The server is entering the primary role. 1. Check the system status by clicking Status Summary screen of Maintenance interface. The Status Summary should show the state primary/ backup. 2. If the server is not in primary/ backup state, escalate the problem to Avaya Services.			
.85	avCCSSrvEntSecondary minor	The server is entering service as the secondary or backup server	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The server is interchanging to the backup role. 1. Check the system status by clicking Status Summary screen of Maintenance interface. The Status Summary should show the state primary/ backup. 2. If the server is not in primary/ backup state, escalate the problem to Avaya Services.			

OID	Object Type	Description	Variables
.86	avCCSSrvTakeover major	The server is taking over as primary server.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The backup server is taking over as the primary. The existing primary server may experience faults. 1. Check the system status with the Status Summary screen of the Maintenance interface. The Status Summary should show the state primary/ backup. 2. If the server is not in primary/ backup state, escalate the problem to Avaya Services.			

Serial link events traps

In a duplex configuration, a serial link connects the two duplicated servers.

OID	Object Type	Description	Variables
.25	avCCSSerialLinkUp warning	The serial link is up.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Informational. Take no action.			
.26	avCCSSerialLinkDown major	The serial link is down.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The serial link between duplexed servers is down. Verify the serial cables and the connection to the port. If the situation persists, contact Avaya Services.			

UPS events traps

If a universal power supply (UPS) is used, these traps alert an administrator when it comes into service, and of any state changes.

OID	Object Type	Description	Variables
.27	avCCSUPSfailover major	UPS is now providing power to the system	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Prepare for power to resume.			
.28	avCCSUPSstatus warning	UPS status has changed	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Informational. Take no action.			

Proxy events traps

These traps indicate proxy events of which an administrator should be aware. The last five indicate software errors.

OID	Object Type	Description	Variables
.32	avCCSProxyRegAccess major	The proxy cannot access the registrar.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
.33	avCCSProxyEvtSrvAccess	The proxy cannot access the event server.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID

OID	Object Type	Description	Variables
.34	avCCSProxyDBAccess minor	The proxy cannot access the database.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
.36	avCCSProxyCMAccess major	The proxy cannot access the TLS trunk to Communicatio n Manager.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
.37	avCCSProxyLinkAccess major	The proxy cannot access the TLS link to Communicatio n Manager or another proxy.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
.38	avCCSProxyUserAuth major	The proxy cannot authenticate a user.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID

Database events traps

The database events are monitored for the traps described here.

OID	Object Type	Description	Variables
.39	avCCSDBStart warning	The database process has started.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Informational. The database process has started.			

OID	Object Type	Description	Variables
.40	avCCSDBStartFailed major	The database process has failed to start.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The database process has failed to start. Users will not receive services. Restart the server and verify that the database is running by checking for this condition on the Alarms screen of the Maintenance interface. The the alarm generated is avCCSDBStartFailed. If the situation persists, contact Avaya Services immediately.			
.41	avCCSDBStop minor	The database process has stopped.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The database process has stopped. If this is due to administrator action, users will not receive service until the database is restarted. If this was not due to administrator action, reboot the server and verify that the database process has started. Look for the avCCSDBStartOK trap or use **ps -u postgres** to check. If the database refuses to start, contact Avaya Services.			
.42	avCCSDBVacuumFailed major	The database vacuum has failed	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The database vacuum has failed. If the situation persists, please contact Avaya Services.			
.88	avCCSDBUpgradeFailed major	The database upgrade failed.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSDBUpgErrorMesg

OID	Object Type	Description	Variables
.89	avCCSDBUpgradeOK minor	The database upgrade was successful.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Informational only.			
.91	avCCSVacuumOK warning	The database vacuum was successful.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Informational only.			

Apache events traps

Both the administration system and PPM (SIP PIM) run on the Apache web server. This web server is monitored by the traps described in this section.

Although the trap `avCCSApacheStart` is an informational trap, the trap `avCCSApacheStop` is a major event.

OID	Object Type	Description	Variables
.43	avCCSApacheStart warning	The Apache web server has started.	sysUpTime, sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Informational. The Linux Service Apache service has started.			
.44	avCCSApacheStartFailed major	The Apache web server has failed to start.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The Apache web server service failed to start. The web service to the SES server is down.			

OID	Object Type	Description	Variables
.45	avCCSApacheStop minor	The Apache web server has stopped.	sysUpTime, sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The Apache web server service is stopped. Apache service is critical component for SES server operation. Resolve: 1. Login as super user and enter **service httpd restart** at the command line. 2. If the httpd service still cannot be started, escalate the problem to Avaya Services.			

Personal Profile Manager events traps

The PPM (SIP PIM) contributes information into the database. These traps indicate PPM access to the database.

Expect the trap `avCCSPPMInitError` to occur during initial installation only.

OID	Object Type	Description	Variables
.46	avCCSPPMDBAccess major	PPM is not able to access the database.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
This event can occur for two reasons: 1. PPM is not able to connect to the database. A single event probably indicates that some element in the system was temporarily out of service, but able to restore itself. If this event repeats constantly, then a more serious problem exists. If PPM is the only element reporting an event indicating that the database is not accessible, try restarting tomcat using the **`service tomcat4 restart`** command from the Linux prompt. If the problem continues, a system error exists that requires additional services support. 2. PPM detected corruption in the database. If the event repeats, inspect the PPM log (/var/log/sip-server/ppm.log or ppm.log.1, ppm.log.2, and so on) for additional information. The problem might be fixed by using the Administration interface to remove the user, as identified by the information in ppm.log, and then add the user back. If not, this problem will likely require additional services support.			
.68	avCCSPPMResourceError major	PPM is not able to access the indicated resource.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSPPMResource

OID	Object Type	Description	Variables
This event may occur for several reasons: 1. The media server running Communication Manager may be momentarily unavailable, perhaps performing reboot. 2. This error may be caused by incomplete information in the database. From the Administration interface, run the **Force All** command. If you recently performed a migration to a higher version level, make sure you have all the fields filled in for the new fields. If the problem continues, additional services support is required. If you run Force All, expect a service outage. 3. PPM obtains a variety of information from associated Communication Manager media servers, and the information might be incorrect. • Go to the Administration interface and check the data on the Edit Media Server screen and the Edit Host screen. Particularly, retype the value for the Profile Service Password on the Edit Host screen. • Go to the **Edit Media Server** screen and make sure that you have stipulated a valid password that is of type `Customer` and service level `superuser` at a minimum. • Also, from the Administration interface, inspect the Media Servers configurations. The address used to communicate with Communication Manager should be that used for administration, not of a CLAN. • Try re-entering the login and password (these must match a SAT login and password on Communication Manager). • Note that in periods of heavy traffic, various elements in the system might shed load to support higher priority tasks. Alarms might reflect this behavior. • If you run **Force All**, expect a service outage. If the problem continues, request additional services support.			
.69	avCCSPPMInitError minor	PPM initialization error has occurred	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSPPMError
This event is generated for these reasons: 1. This event indicates that PPM was not able to decrypt data, likely caused by an internal software error. Additional services support is required. 2. This error indicates that PPM could not read the `ccs.conf` file during initialization, so PPM is not running. Verify that the **ccsConf** parameter found in web.xml (/usr/share/jakarta-tomcat-4.1.27/webapps/axis/WEB-INF/web.xml) points to the `ccs.conf` file, and that permissions on the file allow it to be read. 3. This event indicates that PPM was not able to determine the server's online status during initialization, so PPM is not running. Verify that the **statusCommand** parameter found in web.xml (/usr/share/jakarta-tomcat-4.1.27/webapps/axis/WEB-INF/web.xml) fully qualifies the res-status command that can be executed from the shell to determine server status in a redundant system.			

OID	Object Type	Description	Variables
4. This event indicates that PPM was not able to load the database driver during initialization, so PPM is not running. Verify that the **dbDriveName** parameter found in web.xml (/usr/share/jakarta-tomcat-4.1.27/webapps/axis/WEB-INF/web.xml) specifies the fully-qualified Java class name of the JDBC driver (org.postgresql.Driver). 5. This event indicates that PPM did not obtain the location of its database during initialization, so PPM is not running. Verify that the **DbURL** parameter found in web.xml correctly identifies the location of the SES/PPM database (jdbc:postgresql:mvss).			
6. Inspect the ppm.log and look for more information. This may depend on coding. Additional services support is required. 7. This event indicates that PPM was not able to connect to the database at initialization time, so initialization failed. Verify that postgres is running. Restart tomcat by running the **service tomcat4 restart** command from the Linux prompt.			
8. This event indicates that PPM encountered a fault getting data from the database. The error code was returned by postgres and should help explain the problem. 9. If an SES server restarted, this trap is expected. Otherwise, check ppm.log (/var/log/sip-server/ppm.log, or ppm.log.1, ppm.log.2, etc) for more information. Note that in a redundant system, PPM is restarted on the transition from backup to primary, so this event indicates the server switch over.			
10. This event indicates that PPM was not able to decrypt data, likely caused by an internal software error. Additional services support is required.			
.	avCCSlogResourceError	PPM xxx has occurred.	
	AxisFault remote exception from SMS - SMS Adapter	LOG_SMS_ERROR	
PPM obtains a variety of information from associated Communication Managers. 1. Inspect the PPM log (/var/log/sip-server/ppm.log, or ppm.log.1, ppm.log.2, etc) and the httpd error log (/var/log/httpd/error_log) for additional information, such as the address of the Communication Manager from which PPM was unable to obtain information. 2. From the Administration interface, inspect the Media Servers configurations. The address used to communicate with Communication Manager should be that used for administration, not of a CLAN. 3. Try re-entering the login and password (these must match a SAT login and password on Communication Manager). 4. If the PPM log shows socket read time outs, increase the `smsWaitTime` parameter in the web.xml file (/usr/share/jakarta-tomcat-4.1.27/webapps/axis/WEB-INF/web.xml) and restart Tomcat (using the `service tomcat4 restart` command from the linux prompt). 5. If the problem continues, additional services support is required. Note that in periods of heavy traffic, various elements in the system might shed load to support higher priority tasks. The alarms might reflect this behavior.			
	AxisFault remote exception from SMS - SMSSessionAdapter	LOG_SMS_ERROR	

OID	Object Type	Description	Variables
PPM obtains a variety of information from associated Communication Managers. 1. Inspect the PPM log (/var/log/sip-server/ppm.log, or ppm.log.1, ppm.log.2, etc) and the httpd error log (/var/log/httpd/error_log) for additional information, such as the address of the Communication Manager from which PPM was unable to obtain information. 2. From the Administration interface, inspect the Media Servers configurations. The address used to communicate with Communication Manager should be that used for administration, not of a CLAN. 3. Try re-entering the login and password (these must match a SAT login and password on Communication Manager). 4. If the PPM log shows socket read time outs, increase the `smsWaitTime` parameter in the web.xml file (/usr/share/jakarta-tomcat-4.1.27/webapps/axis/WEB-INF/web.xml) and restart Tomcat (using the `service tomcat4 restart` command from the Linux prompt). 5. If the problem continues, additional services support is required. Note that in periods of heavy traffic, various elements in the system might shed load to support higher priority tasks. The alarms might reflect this behavior.			
	could not create master admin service port	LOG_MAWS_URI_ERROR	
This error may be caused by incomplete information in the database. From master administration, try running the **force all** command. If the problem continues, additional services support is required.			
	malformed URI for master admin service	LOG_MAWS_URI_ERROR	
This error may be caused by incomplete information in the database. From master administration, try running the **force all** command. If the problem continues, additional services support is required.			
	remote exception from master admin service	LOG_MAWS_ERROR	
This error indicates a problem communicating with the master administration service. 1. If the alarm repeats, inspect the PPM log (/var/log/sip-server/ppm.log, or ppm.log.1, ppm.log.2, etc) for additional information about the problem. 2. If the PPM log shows that the socket read timed out, increase the mawsWaitTime parameter in the web.xml file (/usr/share/jakarta-tomcat-4.1.27/webapps/axis/WEB-INF/web.xml) and restart Tomcat (run the command `service tomcat4 restart` from the Linux prompt). 3. For other causes, try running the **force all** command. 4. If the problem continues, additional service support is required.			

OID	Object Type	Description	Variables
.95	avCCSPPMModifiedData minor	PPM has provided reduced or modified data.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID

PPM has been forced to provide dial plan data that have been somehow reduced or modified. Depending on the truncation scheme configured, some dial plan data have been omitted, or each of the terms has been shortened, forcing the client to use an inter-digit timer to determine end of dialing.

Use either of the following remedies:

1. Increase the maximum number of terms that PPM may provide
2. Modify the AAR and ARS analysis tables on Communication Manager to define general rules with specific exceptions.

A sample entry in the alarm log looks like this:

```
605 CCS 95 MIN Y Wed Apr 20 12:43:32 EDT 2005 avCCSPPMModifiedData:
Dialplan was truncated for handle 8896
```

Administration system events traps

These traps monitor the administration system for events that indicate software problems.

OID	Object Type	Description	Variables
.47	avCCSAdminDBAccess major	The administration system cannot access the admin database.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID

The master administration database on a system is inaccessible.

1. Verify the ~postgres/data/pg_hba.conf file for DB permissions.
2. If using DNS, verify that the host name is resolvable and authorized to access the DB as defined in the pg_hba.conf file.
3. Verify that Postgres is running.
4. Verify that the correct host name is administered in /usr/impress/admin/share/impress.ini under the [ImpressDb] section of the file on the affected system.

.48	avCCSAdminRuntimeDBAccess major	The administration system cannot access the runtime database.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID

OID	Object Type	Description	Variables
The runtime database on a home/edge or home system is inaccessible. 1. Verify that the mvss DB password administered during installation matches the DB password administered when the host was added. 2. Verify that Postgres is running on the home/edge or home system. 3. Verify the ~postgres/data/pg_hba.conf file for DB permissions. 4. If using DNS, verify that the host name is resolvable and authorized to access the DB as defined in the pg_hba.conf file. 5. Verify that Postgres is running. 6. Verify that the correct host name is administered in /usr/impress/admin/share/impress.ini under the [ImpressDb] section of the file on the affected system.			
.49	avCCSAdminFailedLogin major	Administrator login has failed.	sysUpTime, sysObjectID, avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
A user trying to log in as **admin** has entered the incorrect password. Verify that the correct password for the admin login is being used.			
.50	avCCSAdminError minor	An administration error has occurred	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
An administration function has raised an error. Examine the appropriate line number of the affected file as specified in the error log message for details.			
.51	avCCSAdminPWCreate Failed major	A password create has failed.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The system was unable to add or update a user's password. Verify that the installation of the admin tools and shared libraries was successful by seeing if /opt/ecsweb/admin/share/bin/epwd exists, and if the /opt/ecs/web/admin/share/lib directory exists and is populated.			

OID	Object Type	Description	Variables
.52	avCCSAdminDBnotCompatible major	The database schema between the edge and home servers are not compatible.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
A **force all** or **update** to a home server has failed because the DB schema version of the master administration database does not match that of the runtime database on a home/edge or edge with homes. This can happen when a system is upgraded, a dbupgrade has occurred and the **import** command is used to restore the system data rather than the **restore** command. Although the system and database may contain the latest DB schema version, the imported data contain an old database schema that causes this error. Do not use the **import** command for a data restore following an upgrade. Data restore following an upgrade should only be done using the **restore** command.			

Registrar events traps

Traps generated from the registrar server indicate software problems

Add a string detailing the username used during authentication failure events.

OID	Object Type	Description	Variables
.57	avCCSRegRegAuthfailed (note the letter G) warning	A registration authentication attempt failed.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
.58	avCCSRegReqAuthfailed (note the Q) warning	An authentication request has failed.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID

Presence server events trap

Traps generated by the presence server indicate software problems.

OID	Object Type	Description	Variables
.59	avCCSPresRegAccess major	The presence server cannot access the registrar.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Restart the event server and Sip Server.			

IM Logger events traps

The traps generated by the IM Logger indicate software problems.

OID	Object Type	Description	Variables
.66	avCCSIMLoggerWarning major	80% of the maximum administered space for IM log files has been reached.	sysUpTime, sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
80% of the maximum administered space for IM log files has been reached. If not corrected, expect to see the trap .67, discussed in the next row.			
.67	avCCSalarmLoggerNoSpace major	The maximum administered space for IM log files has been reached.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The maximum administered space for IM log files has been reached. The system is deleting old log files to make space for newer ones.			

Event server events traps

OID	Object Type	Description	Variables
.70	avCCSEvtSrvDBAccess major	The event server cannot access the database	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
Check the status of the Postgres service using the **service postgresql status** command. Restart the Postgres service if it is stopped.			
.71	avCCSEvtSrvSOAPinitFailed major	The event server failed to initialize the SOAP interface	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
The PPM communication to endpoints must have the SOAP server. Restart the event server. Restart the SES server if the SOAP server still fails to start.			
.72	avCCSEvtSrvSubsRej warning	An endpoint subscription was rejected by the event server.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSEvtSrvReason avCCSEvtSrvPkj
The event server rejected an endpoint subscription request. This could be simply a configuration issue, such as no media server administered for this user, or a security problem where someone who is not allowed is trying to access resources. Check your media servers against the data in the trap.			
.73	avCCSEvtSrvCMSubFailed major	The event server Communication Manager subscription has failed.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSCMHostname avCCSCMIPAddress avCCSalarmType avCCSProductID

OID	Object Type	Description	Variables
The event server subscription to Communication Manager has failed. This trap occurs because of some configuration problem, possibly these: • Communication Manager may not know about the SES system. • Domains are misconfigured. • Domains have incompatible versions of software loaded.			
.74	avCCSEvtSrvCMSubRetry warning	The event server is retrying a subscription to Communication Manager.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSCMHostname avCCSCMIPAddress avCCSEvtSrvPkj avCCSEvtSrvReason avCCSalarmType avCCSProductID
The event server is retrying a subscription to a media server because the media server has not been accessible. This could be because of the network problems or because the Communication Manager was rebooting. Check the network for outages. Wait for Communication Manager to fully reboot.			
.75	avCCSEvtSrvCMPkgNotSupported major	Communication Manager does not support this event package.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSCMHostname avCCSCMIPAddress avCCSEvtSrvPkj avCCSalarmType avCCSProductID
Communication Manager rejected a subscription request because it does not support that event package. Check for incompatible versions of software running on SES servers and Communication Manager.			
.76	avCCSEvtSrvMemError major	The event server does not have sufficient memory resources.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname aavCCSalarmType avCCSProductID
1. Restart the event server. 2. Check the total memory usage on the system using the **top** command and restart the system if the available physical memory is very low.			

OID	Object Type	Description	Variables
.78	avCCSEvtSrvCMResubscribe warning	The event server has received a request from Communication Manager to recreate event server subscriptions to Communication Manager.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSCMIPAddress avCCSEvtSrvPkj aavCCSalarmType avCCSProductID
The event server is trying to renew subscriptions to Communication Manager because of a Communication Manager reboot. When the Communication Manager is fully rebooted, the warnings stop.			

License-related events traps

If a server has a license error, it may impact service, perhaps several days later.

Supporting details for these traps, such as not being able to connect to the WebLM server, are captured in the error log.

OID	Object Type	Description	Variables
.79	avCCSLicErrorMode major	The server is in license error mode.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID avCCSLicErrorMessage
The grace period for the license has been exceeded and service will be suspended for one of the following: • basic license—no proxy service • home seats—the number of exceeded users will be disabled • edge—no edge routing will be performed (no routing out of the domain)			
.80	avCCSNoLicense major	The server has no license.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID

OID	Object Type	Description	Variables
The server could not get a license, but has service due to the grace period. The syslog message and the administration screen message states why the server could not get a license. Advise management to correct the license expiration within the grace period to avoid losing service.			
.81	avCCSLicSeatsExceeded minor	The number of administered seats exceeds the licensed amount.	sysUpTime sysObjectID avCCSIPAddress avCCSHostname avCCSalarmType avCCSProductID
This trap indicates that the number of home seats has been exceeded. Advise management to purchase more home seat licenses.			

Standard MIB support

The SES system also supports the following groups within the IETF (RFC 1213) standard MIB-II:

- System
- IP
- Interfaces

SNMP sets traps or notifications are not supported for MIB-II.

The above MIB-II groups allow network management consoles to recognize each SES server individually as an Avaya IP network element.

Change the community string

1. Log in as root.
2. Edit the `/etc/snmp/snmpd.conf` file and change the string `public` on line 12 to the desired community string.
3. Run the command `service snmpd restart`.

INADS Support

This section contains these topics:

Traps resulting in INADS call

The Global Alarm Manager monitors the following traps, which apply alarm rules to determine when to forward INADS alarm. Traps are sent at the time the event occurs, and again in an hour if the situation persists.

The traps in this list are in alphabetical order.

avCCSAdminDBAccess	avCCSProxyDBAccess
avCCSAdminRuntimeDBAccess	avCCSProxyLinkAccess
avCCSApacheStartFailed	avCCSProxyRegAccess
avCCSApacheStop	avCCSRAID1
avCCSCPUutilization	avCCSDRBDFault
avCCSDBStartFailed	avCCSEthfaultPrivate
avCCSDBStop	avCCSEvtSrvDBAccess
avCCSDiskWarning	avCCSFORestart
avCCSPresRegAccess	avCCSHAfault
avCCSProcessStartFailed	avCCSHBDown
avCCSProcessStop	avCCSIPfailFault
avCCSProxyCMAccess	avCCSMONfault
avCCSSerialLinkUp	avCCSNoDiskSpace
avCCSVIPFault	avCCSPPMDBAccess

MIB object ID

The MIB requires an object ID under the Avaya `sip-prod-mib` subtree. To accommodate this, the MIB is placed in this branch of the Avaya sub-tree:

```
avaya 1.3.6.1.4.1.68889
     mibs (2)
          avSIPMibs (5)
               avCCSMib (1)
```

Index of SNMP traps

Glossary

A

access code — A dial code of 1 digit to 3 digits that activates a feature, cancels a feature, or accesses an outgoing trunk.

Access Security Gateway — See ASG.

alias — An alternative name for an object, such as a variable, file, or device.

ANSI — American National Standards Institute. A professional technical association that supports standards for transmission, protocol, and high-level languages, and that represents the US in the ISO. ANSI standards are for voluntary use in the US.

ART — Auto Registration Tool. ART allows customers and technicians to register newly installed products for warranty and service support.

ASG — Access Security Gateway. A software module that secures Avaya Global Services login accounts on SES servers. Each login attempt on these accounts is met with a one-time challenge string that must be answered with the correct one-time response.

Avaya Communication Manager — An open, scalable, highly reliable, and secure telephony application. Communication Manager provides user functionality and system management functionality, intelligent call routing, application integration and extensibility, and Enterprise Communications networking.

B

B-channel — Bearer channel. A 64-kbps channel or a 56-kbps channel that carries a variety of digital information streams. A B-channel carries voice at 64 kbps, data at up to 64 kbps, WebLM voice encoded at 64 kbps, and voice at less than 64 kbps, alone or combined. See also D-channel.

backup — In a duplex configuration supporting local failover, this is the server that is synchronized and ready to interchange with the primary server. Sometimes referred to as the secondary.

bus — A multi-conductor electrical path that transfers information over a common connection from any of several sources to any of several destinations. *See also* packet bus.

C

carrier — An enclosed shelf that contains vertical slots that hold circuit packs.

CDR — Call detail record. A file that uses software and hardware to record call data. CDR was formerly called Station Message Detail Recording (SMDR). *See also* CDRU.

CDRU	Call detail recording utility. Software that collects, stores, filters, and provides output of call detail records. *See also* CDR.
channel	1. A circuit-switched call. 2. A communications path that transmits voice and data. 3. In WebLM transmission, all the contiguous time slots or non-contiguous time slots that are necessary to support a call. For example, an H0-channel uses six 64-kbps time slots. (4) A digital signal-0 (DS0) on a T1 facility or an E1 facility that is not specifically associated with a logical circuit-switched call. *See also* D-channel.
circuit	1. An arrangement of electrical elements through which electric current flows. 2. A channel or a transmission path between two or more points.
circuit pack	A circuit card on which electrical circuits are printed, and integrated circuit (IC) chips and electrical components are installed. A circuit pack is installed in a SSH carrier. One example is the TN2302.
CCITT	Comitte Consultatif International Telephonique et Telegraphique. *See* ITU.
CCS	See SES.
CLAN circuit pack	Controlled local area network. A circuit pack (TN799B) in an Avaya DEFINITY port network (PN) that provides TCP/IP connectivity to adjuncts over Ethernet or PPP. The CLAN circuit pack serves as the network interface for a DEFINITY server. The CLAN terminates IP (TCP and UDP), and relays those sockets and connections up to the Avaya DEFINITY server.
CO	Central office. Telephone switching equipment that provides local telephone service and access to toll facilities for long distance calling.
Communication Manager	Avaya Communication Manager., An open, scalable, highly reliable, and secure telephony application. Communication Manager provides user functionality and system management functionality, intelligent call routing, application integration and extensibility, and Enterprise Communications networking.
communications system	A software-controlled processor complex that interprets dial pulses, tones, and keyboard characters, and makes the proper connections within the system and externally. The communications system consists of a digital computer, software, storage devices, and carriers, with special hardware to perform the connections. A communications system provides communications services for the telephones on customer premises and the data terminals on customer premises, including access to public networks and PPPs. *See also* SSH.
Converged Communications Server (CCS)	See SES.
COR	Class of Restriction. A feature that allows up to 96 classes of call-origination restrictions and call-termination restrictions for telephones, telephone groups, data modules, and trunk groups. *See also* COS.

COS Class of Service. A feature that uses a number to specify whether telephone users can activate the Automatic Callback (ACB), Call Forwarding All Calls, Data Privacy, or Priority Calling features. *See also* COR.

CPN Called-party number.

CPN/BN Calling-party number/billing number.

CPE Customer premises equipment. Equipment that is connected to the telephone network, and that resides on a customer site. CPE can include telephones, modems, fax machines, video conferencing devices, switches, and so on.

D

D-channel Data channel. A 16-kbps channel or a 64-kbps channel that carries signaling information or data on an ISDN-BRI or ISDN-PRI. *See also* B-channel.

data module An interconnection device between a Basic Rate Interface (BRI) or a digital communications protocol (DCP) interface of the SSH, and the DTE or D-channel.

data terminal An input/output (I/O) device that has either switched access or direct access to a host computer or to a processor interface.

DCE Data communications equipment. Equipment on the network side of a communications link that makes the binary serial data from the source or the transmitter compatible with the communications channel. DCE is usually a modem, a data module, or a PAD.

DCHP Dynamic host configuration protocol. An IETF protocol (RFCs 951, 1534, 1542, 2131, and 2132) that assigns IP addresses dynamically from a pool of addresses instead of statically. DHCP provides the IP address to the SIP device.

DCP Digital communications protocol. A proprietary protocol that transmits both digitized voice and digitized data over the same communications link. A DCP link consists of two 64-kbps information (I) channels, and one 8-kbps signaling (S) channel. The DCP protocol supports two information-bearing channels, and thus two telephones or data modules. The I1 channel is the DCP channel that is assigned on the first page of the 8411 Station screen. The I2 channel is the DCP channel that is assigned on the analog adjunct page of the 8411 Station screen, or on the data module page.

digital The representation of information by discrete steps. Compare with *analog*.

DIMM Dual Inline Memory Module.

DNS Domain name service. a system that stores information about host names and domain names in a kind of distributed database on networks, such as the Internet. DNS provides an IP address for each host name, and lists the mail exchange servers accepting e-mail for each domain.

DRBD Distributed redundant block device.

DTE Data terminal equipment. Equipment that comprises the endpoints in a connection over a data circuit. In a connection between a data terminal and a host, the terminal, the host, and the associated modems or data modules comprise the DTE.

DTMF Dual-tone multifrequency. The touchtone signals that are used for in-band telephone signaling.

duplex The host configuration supporting local failover by using the interchange of the primary and backup servers. Any host node may comprise two interconnected servers. Compare with simplex.

E

edge In Avaya's SIP architecture, this is the proxy server that forwards requests to and from the customer's network. It sends inbound SIP requests or messages to the home proxy servicing the specified user.

extension A number from 1 digit to 5 digits that routes calls through a communications system. With a Uniform Dial Plan (UDP) or a main-satellite dialing plan, extensions also route calls through a PPP.

F

FTP File Transfer Protocol.

FQD or FQDN Fully qualified domain name. A fully qualified domain name consists of a host and domain name, including top-level domain, for example, `Bill.Gates@MSN.com`.

H

H.323 An ITU standard for switched multimedia communication between a LAN-based multimedia endpoint and a gatekeeper. *See also* SIP.

HAP High availability platform.

handle A handle is the way SES and Communication manager recognize an end user, or perhaps a group. A handle could be an end user's telephone extension, real name, a nickname, or a designation. Handles may have two URIs available for contacting the end user, perhaps a DID extension, or an email address.

home This is the domain providing service to a SIP user, used in registering that user with a home proxy. A home server is designated generally as a host, and the series of Host screens administer it.

host name See FQD or FQDN.

host computer A computer that is connected to a network, and that processes data from data entry devices. In SES, a host is an S8300, or an S8500 (x306 or x305). In addition, a host holds either the edge server, the home server, or acts as a combined home/edge. Contrast with media server.

I

ICMP Short for Internet Control Message Protocol, an extension to the Internet Protocol (IP) defined by RFC 792. ICMP supports packets containing error, control, and informational messages. The **`ping`** command, for example, uses ICMP to test an Internet connection.

IETF Internet Engineering Task Force. One of two technical working bodies of the Internet Activities Board. The IETF develops new TCP/IP/IP standards for the Internet.

IM Instant Messaging. The instant-messaging client software required for release R3.0 of Avaya SES is a version of the Avaya IP Softphone R5 or later, or SIP Softphone R2 or later.

interchange Term used for when the primary server in a duplex configuration relinquishes control and its backup server takes over that control, running the SIP software applications and services for this SES node.

IP Internet protocol. A connectionless protocol that operates at layer 3 of the OSI model. IP protocol is used for Internet addressing and routing packets over multiple narrowbands to a final destination. IP protocol works in conjunction with TCP/IP/IP.

ISDN Integrated Services Digital Network. A public network or a PPP that provides end-to-end digital communications for all services to which users have access. An ISDN uses a limited set of standard, multipurpose, user-network interfaces that are defined by the CCITT. Through internationally accepted standard interfaces, an ISDN provides digital circuit switching communications or packet switching communications within the network. An ISDN provides links to other ISDNs to provide national digital communications and international digital communications. *See also* ISDN-BRI, ISDN-PRI.

ISDN-BRI Integrated Services Digital Network Basic Rate Interface. The interface between a communications system and terminal that includes two 64-kbps B-channels for transmitting voice or data, and one 16-kbps D-channel for transmitting associated B-channel call control and out-of-band signaling information. ISDN-BRI also includes 48 kbps for transmitting framing and D-channel contention information, for a total interface speed of 192 kbps. ISDN-BRI serves ISDN terminals and digital terminals that are fitted with ISDN terminal adapters. *See also* ISDN-PRI.

ISDN-PRI Integrated Services Digital Network Primary Rate Interface. The interface between multiple communications systems that in North America includes 24 64-kbps channels that correspond to the North American digital signal-level 1 (DS1) standard rate of 1.544 Mbps. The most common arrangement of channels in ISDN-PRI is 23 64-kbps B-channels for transmitting voice and data, and one 64-kbps D-channel for transmitting associated B-channel call control and out-of-band signaling information. With nonfacility-associated signaling (NFAS), ISDN-PRI can include 24 B-channels and no D-channel. *See also* ISDN, ISDN-BRI.

ISO International Organization for Standards. A worldwide federation of standards bodies who issue International Standards for technological, scientific, intellectual, and economic activity. The federation is called *ISO*, and the US representative to the federation is the ANSI.

ITU International Telecommunications Union. An international organization that sets universal standards for data communication, including ISDN. ITU was formerly known as International Telegraph and Telephone Consultative Committee (CCITT).

L

LAN Local area network. A networking arrangement that is designed for a limited geographical area. Generally, a LAN is limited in range to a maximum of 6.2 miles, and provides high-speed carrier service with low error rates. Common configurations include daisy chain, star (including circuit-switched), ring, and bus.

local failover The feature supports database replication and interchange, as needed, between two servers (one primary, one backup), which are connected in a duplex configuration.

M

MAC MAC address or MAC name. Media Access Control address, a 48-bit hardware address that uniquely identifies each node, interface card, or device of a network.

media server 1. In SES specifically, a media server refers to the Linux-based hardware on which Avaya Communication Manager has been installed. This media server must have a map to a CSS host, home or edge, to access and deliver SES features.

2. Avaya Media Server. A family of application-enabling processing platforms based on open CPUs and industry-standard operating systems. Media servers provide multiprotocol networking that includes, but is not limited to, Internet Protocol (IP). In addition to supporting a highly diversified network architecture, media servers provide user functionality, system management functionality, intelligent call routing, application integration, mobility, and conferencing.

MIB Management information base. A directory listing logical names of resources on a network, pertinent to the network's management.

N

narrowband A circuit-switched call at a data rate of 64 kbps or less. All switch calls that are not WebLM are considered to be narrowband. *Compare with* wideband.

network A series of points, nodes, or stations that are connected by communications channels.

NIC Network Interface Card.

node A switching point or a control point for a network. Nodes are either tandem or terminal. Tandem nodes receive signals and pass the signals on. Terminal nodes originate a transmission path or terminate a transmission path.

O

OSI Open Systems Interconnect. A system of seven independent communication protocols defined by the ISO or ISO. Each of the seven protocols enhances the communications services of the layer below, and shields the layer above from the implementation details of the lower layer. In theory, this structure can be used to build communications systems from independently developed layers.

P

packet A group of bits used in packet switching and transmitted as a discrete unit. A packet includes a message element and a control information element (IE). The message element is the data. The control IE is the header. In each packet, the message element and the control IE are arranged in a specified format.

PAD Packet assembly/disassembly. The process of packetizing control data and user data from a transmitting device before the data are forwarded through the packet network.The receiving device disassembles the packets, removes the control data, and then reassembles the packets, reconstituting the user data in original form.

packet bus A bus with a wide bandwidth that transmits packets.

packet switching A data-transmission technique that segments and routes user information in discrete data envelopes that are called *packet*s. Control information for routing, sequencing, and error checking is appended to each packet. With packet switching, a channel is occupied only during the transmission of a packet. On completion of the transmission, the channel is made available for the transfer of other packets.

PBX Private Branch Exchange. *See* SSH.

PCI PC interface (card).

PDU

In telecommunications, the term protocol data unit (PDU) has the following meanings:

1. Information that is delivered as a unit among peer entities of a network and that may contain control information, address information, or data.

2. In layered systems, a unit of data that is specified in a protocol of a given layer and that consists of protocol-control information of the given layer and possibly user data of that layer.

Source: from Federal Standard 1037C

POTS Plain Old Telephone Service. Basic voice communications with standard, single-line phones accessing the PSTN.

PPM Personal Profile Manager. This is the portion of the SIP interface that lets the end user manage their demographic data.

PPP Point-to-Point Protocol. A standard that largely replaces SLIP, allowing a computer to use TCP/IP with a regular telephone line.

port A data-transmission access point or voice-transmission access point on a device that is used for communicating with other devices.

primary In a duplex configuration supporting local failover, this is the server that is running the SIP applications and services. Sometimes referred to as the active server, server A, or others. Compare with backup.

private network A network that is used exclusively for the telecommunications needs of a particular customer.

protocol A set of conventions or rules that governs the format and the timing of message exchanges. A protocol controls error correction and the movement of data.

proxy server An intermediary client/server entity for making requests on behalf of other client entities. The job of an Avaya SIP proxy is to ensure that a request is sent to the entity closest to the specified user. For example, an edge proxy server interprets and forward requests intended for specific users to their particular home proxy servers.

PSTN Public Switched Telephone Network.

public network A network to which all customers have open access for local calling and long distance calling.

PSTN Public switched telephone network. The public worldwide voice telephone network.

R

RAS Remote Access Server or, in Microsoft Windows operating systems, Remote Access Service.

RFA Remote Feature Activation is a web-based application that obtains Avaya authentication and licensing files. The home page for this application is at http://rfa.avaya.com.

RNIS Remote Network Implementation Services is a contract installation services group within Avaya Inc.

RPM RedHat Package Manager.

RSA Remote Supervisor Adapter. This module is in the S8500 server and acts as a remote servicing module. See SAMP.

RTC Real Time Communication.

RTCP Real Time Control Protocol.

RTP Real time transfer protocol. An IETF protocol (RFC 1889 and 3550) that addresses the problems that occur when video and other exchanges with real-time properties are delivered over a LAN that is designed for data. RTP gives higher priority to video and other real-time interactive exchanges than to connectionless data.

S

SAMP Server Availability Management Processor. This module is in the S8500 server and acts as a remote servicing module. See RSA.

SOAP Simple Object Access Protocol is a light-weight protocol for exchanging messages between computer software, typically in the form of software componentry. The word object implies that the use should adhere to the object-oriented programming paradigm.

SOAP is an extensible and decentralized framework that can work over multiple computer network protocol stacks. Remote procedure calls can be modeled as an interaction of several SOAP messages. SOAP is one of the enabling protocols for Web services.

SOAP can be run on top of all the Internet Protocols, but HTTP is the most common and the only one standardized by the W3C. SOAP is based on XML, and its design follows the Head-Body software pattern, like HTML. The optional **Header** contains meta-information such as information for routing, security, and transactions. The **Body** transports the main information, sometimes known as the payload. The payload is compliant with an XML Schema.

secondary Another name for the backup server, or server B, in a duplex configuration. Compare with primary.

SES **SIP Enablement Services** Formerly, Converged Communications Server. Avaya's proxy server for SIP, supporting instant messaging using the client in Avaya IP Softphone R5 or later, or SIP Softphone R2 or later, and voice communication using Avaya 46xxSIP phones.

SIP Session initiation protocol. An IETF standard (RFC 3261) signaling protocol for Internet conferencing, telephony, presence, events notification, and instant messaging. SIP initiates call setup, routing, authentication, and other feature messages to endpoints within an IP domain. *See also* H.323, VoIP.

simplex An SES host configuration with one server/database per node. Compare with duplex.

SMS Short for Short Message Service. Similar to paging, SMS is a service for sending short text messages to mobile phones.

SNMP Simple Network Management Protocol.The industry-standard protocol that governs network management and the monitoring of network devices and the functions of those devices. The user of SNMP is not necessarily limited to TCP/IP networks, but can be implemented on Ethernet and Open Systems Interconnect (OSI) transports.

SSH Secure SHell is a protocol for secure remote login and other secure network services over an unsecure network. It provides for server authentication and data integrity with perfect port-forwarding secrecy.

SSG Secure Services Gateway. The SSG is an Avaya server installed within a DMZ on the customer's network. It terminates the customer end of a secure link, such as VPN or frame relay, to Avaya remote servicing tools. In the inbound direction, the SSG provides secure remote access to multiple Avaya products on the customer's network, making detailed audit logs and full administrative control available to the customer. In the outbound direction, the SSG collect INADS SNMP alarms from multiple Avaya products and forwards them to alarm receivers on the Avaya network.

subscriber A SIP subscriber (end user) is one of the following: an SES R3.0 host or other SIP node, a SIP user, or a media server (running Avaya Communication Manager R3.0 or later for SES R3.0).

switch Any kind of telephone switching system. *See also* communications system.

T

TAC Trunk access code. A dial access code used to access a specific trunk.

TCP Transmission Control Protocol. A connection-oriented transport-layer protocol, IETF STD 7. RFC 793, that governs the exchange of sequential data. Whereas the IP deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data, and also guarantees that packets are delivered in the same order in which the packets are sent.

TCP/IP *See* IP. *See also* TCP.

tie trunk A telecommunications channel that directly connects two private switching systems.

TLS Transport Layer Security. An IETF standard (RFC 2246) to supersede Netscapes' Secure Socket Layer (SSL) and provide host-to-host data connections with encryption and certification at the transport layer, as the name implies.

TSP Toshiba SIP Phone.

trunk A dedicated communications channel between two communications systems or COs.

trunk group Telecommunications channels that are assigned as a group for certain functions, and that can be used interchangeably between two communications systems or COs.

U

UDP

1. User datagram protocol. A packet format that is included in the TCP/IP suite of protocols. UDP is used for the unacknowledged transmission of short user messages and control messages.

2. Uniform Dial Plan.

Unicode

UTF-8, shift JIS, Asian character set, multibyte languages.

URI

Uniform resource identifiers. URIs (also called URLs) are short strings of characters that identify resources on the world-wide web. They make resources available under a variety of naming schemes and access methods such as HTTP, FTP, SIP, and Internet mail in the same way.

USB

Universal serial bus. A high-speed serial interface used to add a printer, a modem, a keyboard, a mouse, or another peripheral device to a personal computer.

V

VMM

VoIP Monitoring Manager. This application checks with the endpoint device, perhaps every 5 seconds or so, to check the quality of service on the device. VMM is administered on the Add Host screen and other Host screens in CSS.

VMON

Voip Monitoring. See VMM.

VoIP

Voice over IP. A set of facilities that use the IP to manage the delivery of voice information. In general, VoIP means to send voice information in digital form in discrete packets instead of in the traditional circuit-committed protocols of the PSTN. Users of VoIP and Internet telephony avoid the tolls that are charged for ordinary telephone service.

W

WebLM

Web-based License Management, a server application that manages various software licenses.

wideband

A circuit-switched call at a data rate that is greater than 64 kilobits per second. A circuit-switched call on a single T1 facility or a single E1 facility with a bandwidth that is between 128 kilobits per second and 1536 kilobits per second (T1) or 1984 kilobits per second (E1) in multiples of 64 kilobits per second. H0, H11, H12, and N x digital signal-level 0 (DS0) calls are wideband. Compare with narrowband.

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W