Converged Communications Server

Release 2.1

Installation and Administration

555-245-705
Issue 2.1
November 2004

Notice

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

Warranty

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

Preventing Toll Fraud

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

Avaya Fraud Intervention

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

How to Get Help

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

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

Providing Telecommunications Security

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

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

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

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

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

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

Responsibility for Your Company's Telecommunications Security

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

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

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

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

TCP/IP Facilities

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

Standards Compliance

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

Product Safety Standards

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

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

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

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

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

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

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

The LASER devices operate within the following parameters:

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

Luokan 1 Laserlaite

Klass 1 Laser Apparat

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

Electromagnetic Compatibility (EMC) Standards

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

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

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

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

Federal Communications Commission Statement

Part 15:

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

Part 68: Answer-Supervision Signaling

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

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

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

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

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

REN Number

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

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

For G350 and G700 Media Gateways:

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

For all media gateways:

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

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

Means of Connection

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

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

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

For G350 and G700 Media Gateways:

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

For all media gateways:

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

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

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

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

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

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

Canadian Department of Communications (DOC) Interference Information

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

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

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

Declarations of Conformity

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

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

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

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

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

European Union Declarations of Conformity

CE

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

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

Japan

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

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

To order copies of this and other documents:

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

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

E-mail: totalware@gwsmail.com

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

Contents

1 Introduction

This chapter describes Avaya Converged Communications Server (CCS), what it is and what it does.

Introduction to the Server

What is Converged Communications Server?

An Avaya Converged Communications Server (CCS) is dedicated to performing 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).)

When a release 2.1 Converged Communications Server is set up to communicate with one or more Linux-based media servers running Avaya Communication Manager 2.1.1 or later, then the SIP proxy server supports communication among the various non-SIP endpoints supported by Communication Manager (analog, DCP or H.323 stations and analog, digital or IP trunks) and new SIP-enabled endpoints, such as the Avaya 4602 SIP Telephone and Avaya IP Softphone Release 5.07 and later. SIP-enabled endpoints register with the Avaya proxy; also, they can be managed by Avaya media servers (optionally). In addition, the proxy server supports the SIP-enabled Instant Messaging application between users of IP Softphone R5 client software; for voice, the clients also must be logged in to and managed by Avaya media servers.

How does this server fit into your system?

In addition to the CCS, the support for SIP built into Avaya Communication Manager has the following attributes which help it fit easily into your system:

- It is built around open-source software and published standards (e.g., Linux, SIP and H.323).
- It integrates traditional circuit-switched interfaces and IP-switched interfaces. This integration allows the user to evolve easily 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.

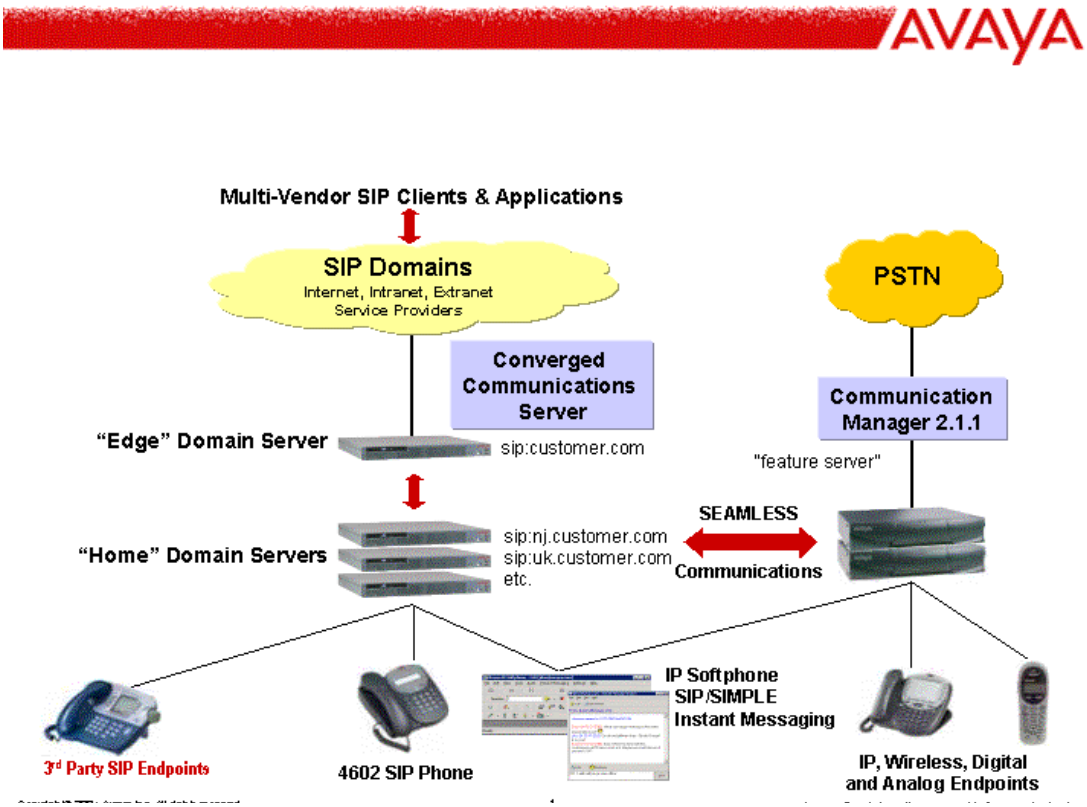
> **NOTE:**
> Building SIP support into Avaya MultiVantage™ software adds another element to the modular family of Avaya components, which seamlessly delivers a business's voice and messaging capabilities over an IP network. Avaya continues enhancing the value it provides to customers in a standards-based, IP communications infrastructure.

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 2.x. A media server running Communication Manager becomes, in effect, a telephony feature server, which is accessible from any SIP endpoint and provides access transparently to many telephony features that the SIP standard currently does not address.

System Architecture

Avaya's SIP architecture supports Converged Communications Servers of different types.

Illustration



Types of CCS Hosts

Edge

The Edge server handles SIP requests from all domains, forwarding requests received from Home servers. If an Edge server is used, then one or more Home servers must also exist in this architecture. Only one Edge server (or combined Home/Edge server) is allowed for any one domain; for example, one Edge server forwards requests to and from the "customer.com" domain.

Home

A Home server handles 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 ten Home servers and exactly one Edge server is required in this scenario. For example, a customer might have one Home server for users@nj.customer.com and another Home for users@uk.customer.com within its network.

Home/Edge

A combined Home/Edge server performs the functions of both a Home server and an Edge server for an enterprise. This is a single-server scenario; that is, no other Home or Edge servers may exist in this architecture.

NOTE:
It is best to architect your system (i.e., a combined server, or multiple servers) with scalability in mind, as this release does not support non-disruptive database migration.

Administrative Interfaces

Master

A proxy server with the web-based Master Administrator interface (typically, an Edge server) supports the updating of 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 interface supports administering both users and media server extensions. Avaya highly recommends you install the Master Administrator interface on the Edge server (or the combined Home/Edge server). Only one server in a CCS system may have the Master interface; other servers have Limited interfaces only.

Limited

A proxy server with the Limited Administrator interface installed on it (typically, a Home server) does not support administering users or their extensions, and cannot update the databases on other servers. But you can administer Maintenance items for the server, for example, and also view a list of registered SIP users on this Home server using the web-based Limited Administrator interface.

Local Failover Feature

An optional new feature in CCS Release 2.1 is Local Failover. This feature supports replicating the CCS database and server software for any particular system node (home, edge, or combination home/edge).

Duplex servers

The Local Failover feature requires a duplex server configuration; since the feature is an option and not mandatory, this means that both the simplex configuration supported in release 2.0.x and the new duplex server configuration (2.1.x) are now supported.

Duplex server is essentially an add-on component to a standard simplex CCS system, and does not require significant differences among other components (except for the addition of dual NIC modules in each server) or any other custom hardware for the two configurations, apart from cabling. Note that all nodes in an enterprise's CCS system do not need to be duplex. For example, in configurations with a separate Edge and (one to ten) Home nodes, duplex servers may be implemented only for the Edge system. In this example, each Home node may remain a simplex server.

Node-level duplication

In this design, a node may be simplex or duplex. In a CCS system, a Home or Edge proxy may reside on two boxes, whose separate power, disk, and communications components make simultaneous failure unlikely. One box is Active and provides service, while the other one (the Standby server) monitors the Active server and takes over if it fails. The Active server performs extensive self-diagnostics as it provides service, voluntarily relinquishing control to the Standby server in case it finds trouble. After giving up control (whether voluntarily or not), the box attempts to restore itself to a state in which it can provide service. Once this has been accomplished (either automatically or via some form of manual intervention), the box then assumes the role of the new Standby 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 active/standby servers and database local failover feature include:

- Health monitoring in the Active server
- Monitoring of the Active server by its Standby server
- Mirroring on the servers of persistent data
- Recovery after failure of the Active 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 Standby server.

Failover scenarios

There are four basic scenarios in which an individual CCS host may fail to process requests:

- An Active server detects its own failure or is taken out of service. It will failover to the Standby server, which will become Active. This exchanging of roles is called "interchange." The server that had been Active tries to become the Standby server, restarting if necessary.
- A Standby server fails or is taken out of service. In this scenario, no "interchange" between the two servers occurs. The Active server maintains normal operation without service interruption. The Standby server may or may not successfully restart itself; if it does, it will remain as Standby.
- An Active server detects a communication problem with its request link. Communication data is shared by the two servers, and if the Standby server detects no problem with its request link, then an interchange will take place. The server that had been Active will restart as the Standby server.
- A Standby server detects the loss of the Active server. It will "interchange" with the Active server, as well as then trying to force the other server to restart as the new Standby server.

Causes for failover

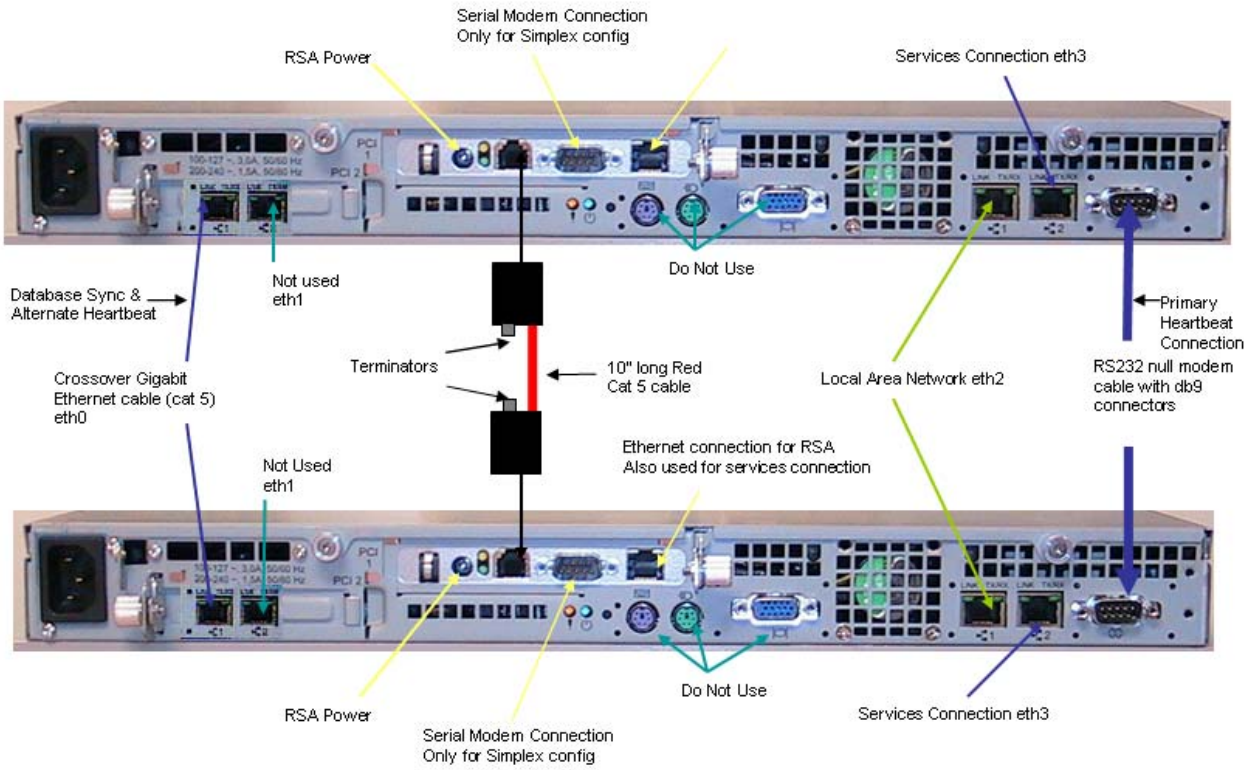
There are a number of reasons that an Active server will choose to interchange with its Standby:

- The Active server cannot communicate via ethernet port eth2, but can communicate with it's Standby server via eth0. If the Standby server can communicate via eth2, it will interchange and become the new Active server.
- Data disk space is 98 percent full.
- One or more of the following server processes on the Active server is down:
  - Alarm process
  - Watchdog daemon
  - Heartbeat service
  - PostgreSQL service.
- Virtual (logical) IP addressing fails to operate.
- RAID 1 (disk mirroring) fails to operate.
- Any required system process on the Active 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 (Active) machine but no error on its partner (the Standby server).

Server interconnections

The following are the ports and cabling that connect duplex servers to each other and to the network:

This Port is the...	And is used for...	And it needs a...
first of the native NIC (eth0 on simplex server, eth2 on duplex servers)	Main IP services	Link to enterprise network using a static IP address for server and a DNS name
second of native NIC ("2") (eth1 on simplex server, eth3 on duplex servers)	Avaya Services	Fixed IP address=192.11.13.6
eth port of RSA card	Avaya Services	Same fixed IP as above (192.11.13.6)
ASM RS-485 port of RSA card	Duplex- server resets	RS-485 adapter with termination and cable to other RS-485 adapter
Serial port native on back, right-hand side of x305	Duplex server communications	RS-232 link between servers (IP information not applicable)
first of add'l dual NIC (N/A to simplex server, eth0 on duplex servers)	Redundant services	Cat5 cross-connect RJ-45 cable between duplex servers and using a fixed IP address of 192.11.14.10 (Active, A) or 192.11.14.11 (Standby, B)
second of add'l dual NIC (N/A to simplex server, eth1 on duplex servers)	Unavailable for use (not configured)	_____



Requirements for the SIP solution

Hardware

The server hardware required for an Avaya Converged Communications Server Release 2.1 is the IBM e-server xSeries 305, hereafter referred to as the x305. 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 a CCS. Instead, you must use the Avaya CCS Setup/Install CD.

An IBM Installation Guide is provided with the x305 and includes instructions for installing the IBM Remote Supervisor Adapter (RSA) module (which you should verify has the latest Avaya RSA firmware) on page 7 of the guide and for installing the dual inline memory module (DIMM) on page 10. ***Note this memory must be added before use.*** To be used as a Converged Communications Server, the x305 needs one additional 512MB DIMM of PC2100 266MHz CL2.5 ECC DDR SDRAM added to the existing 512MB installed by default, to yield a total installed RAM of 1GB.

Before beginning to install any software, you must first disable the RSA loader watchdog. For detailed procedures, refer to page 40 in *Installing and Configuring the Avaya S8500 Media Server*, Doc ID 03-300143. For procedures on verifying and updating the RSA firmware, refer to page 59 in *Upgrading Software and Firmware—Avaya S8500 Media Server,* Doc ID 555-245-111, Issue 2, and to the *Job Aid: Replacing the RSA*, Doc ID 555-245-759, and *The Avaya RSA User's Guide*, Doc ID 555-245-702.

If you are installing a duplex system, then an additional, Intel ProShare dual Network Interface Card (NIC) also must be installed in each server. For detailed procedures, refer to page 49 in *Installing and Configuring the Avaya S8500 Media Server*, Doc ID 03-300143, and to the *Job Aid: Replacing the Dual Network Interface*, Doc ID 555-245-760.

Avaya requires one universal serial bus (USB) modem be connected to each x305 server (one for each of the duplex servers) for remote access. A 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 x305 ships with a blank, unpartitioned hard-disk drive, and without an operating system or any Avaya server software files installed. These must be installed and configured properly before CCS use. Refer to Chapter 2, “Setup and Configuration” in this document for detailed procedures.

In addition, the IP connectivity must be configured correctly on all Avaya Media Server(s) 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

Several software components are installed from the Avaya CCS software CD, including:

- Linux
- 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).

CCS Release 2.1 support is in the 2.1.1 and later releases of Avaya Communication Manager running on any one of the Linux-based media servers (e.g., the Avaya S8700, S8500 or S8300 Media Server).

Firmware

Refer to the *SIP Support in Avaya Communication Manager* document for more details on what firmware vintages are required in certain Avaya products to ensure interoperability in a SIP environment.

NOTE:
BIOS and/or firmware updates should be obtained only through Avaya Inc., or from its authorized BusinessPartners. You should never obtain server updates directly from IBM.

Note that the RSA module has three firmware packets, all of them separate from the x305 server in which it is installed. In addition, the x305 server has a BIOS supplied by Avaya (e.g., build level PLJH61AUS). For more details on firmware, refer to the Avaya Support website at http://www.avaya.com/support

Related Systems

Refer to the *SIP Support in Avaya Communication Manager* document for more details on media server administration requirements for SIP. Refer to the documentation and online help files which came with your Avaya IP SoftPhone R5.1 and/or Avaya 4602 SIP Telephone for details on the client hardware requirements for using Instant Messaging (through the former) and SIP voice calling (through the latter).

For more infomation about the support provided in Avaya's SIP solution for third-party endpoints, see the Application Notes contained within the Resource Library on Avaya's DevConnect website: http://www1.avaya.com/enterprise/resourcelibrary/applicationnotes/devconnect_network.html

2 Setup and Configuration

Configuring a New Server

This section details the variety of tasks involved in installing an Avaya Converged Communications Server for the first time. See Upgrading an Existing Server on page 38 for an R2.0.1 to R2.1 migration.

Initial Assembly and Setup

All Converged Communications Servers (the SIP proxy servers) must be properly connected and configured on an enterprise's IP network. In addition to installing memory, verifying and updating (if needed) the RSA module's firmware (described on page 59 in *Upgrading Software and Firmware—Avaya S8500 Media Server,* Doc ID 555-245-111, Issue 2, and in *The Avaya RSA User's Guide*, DocID 555-245-702, and the *Job Aid: Replacing the RSA*, 555-245-759), the following information will be needed, and must be available before beginning to install the software on the server:

- Host name of each server(s)
  - For a simplex server configuration, one host name is required
  - For a duplex server configuration, one physical host name is required for each of the two servers, as well as another logical name to refer to the duplex system.
- DNS Domain name
- IP address of server(s)
  - For a simplex server configuration, one physical IP address is required
  - For a duplex server configuration, one physical IP address is required for each of the two servers, as well as a unique, logical IP address to refer to the duplex system.
- Net mask
- IP address of the default gateway
- IP address of one, two or three servers running DNS (these must be properly configured if fully qualified domain names are to be used on CCS Setup screens)
- Host name, IP address, net mask and default gateway address of the RSA eth port on this server. For a duplex server configuration, a set of these values is required for each server's RSA module; defaults are supplied which are based off of each server's physical host name.
- IP address of an existing server (typically, an Edge server) running the Master Administrator interface, if you are not installing the Master Administrator interface on this server.

For endpoints on Avaya Communication Manager to interoperate through the CCS, SIP trunking must be administered properly in Communication Manager. (Refer to *SIP Support in Avaya Communication Manager* for more details.) This administration includes, but isn't necessarily limited to, specifying the:

- 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.

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

Installation of Server Software

To install a Converged Communications Server, Avaya's SIP proxy server, the following tasks must be performed locally (usually by an Avaya or BusinessPartner installer):

Verify hardware, firmware and BIOS: - Verify that all the required hardware and cabling connections are present (for both servers, if you are installing a duplex pair), as follows:

1. The x305 contains an RSA module and its firmware has been updated, if needed. For procedures on verifying and updating the RSA firmware, refer to page 59 in *Upgrading Software and Firmware—Avaya S8500 Media Server,* Doc ID 555-245-111, Issue 2, and to the *Job Aid: Replacing the RSA*, Doc ID 555-245-759, and *The Avaya RSA User's Guide*, Doc ID 555-245-702. Also, the RSA power cord should be plugged into an external power source (and not into that of the x305).
2. Before beginning to install any software, you must first disable the RSA loader watchdog. Refer to "Configuring the media server" in Chapter 2 of *Installing and Configuring the Avaya S8500 Media Server*, Doc ID 03-300143, for detailed procedures for disabling the RSA loader watchdog.
3. 1GB RAM has been properly installed (see Hardware on page 26) and enabled in the x305 BIOS.
4. Ensure that the x305 has been upgraded to Avaya BIOS (61A or an approved later release) and that the CD drive is set in that BIOS as the first choice of system boot device.
5. If this server is one of a duplex server set, then ensure that the additional, dual NIC has been installed. For detailed procedures, refer to page 49 in *Installing and Configuring the Avaya S8500 Media Server*, Doc ID 03-300143, and to the *Job Aid: Replacing the Dual Network Interface,* Doc ID 555-245-760.

CAUTION:
Ensure 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 x305 server will indicate hardware alarms associated with it.

Connect Services laptop/PC - Connect the laptop/PC used to perform services to the Avaya Services eth port on the back of the x305 (usually labeled "2") via a category 5 or better cross-connect RJ-45 cable. Set the IP address of the laptop/PC to 192.11.13.5 and use a netmask of 255.255.255.252. No default gateway need be specified.

Install the contents of the CD, beginning with the x305 powered off, as follows -

1. Insert the installation CD in the drive and restart the x305 by recycling AC power. Allow the x305 server to boot from the CD. Once Linux loads into RAM, the Avaya Services port will be ready (typically, in less than 3 minutes).
2. Prompts should be displayed with selections addressing what you want to do (Install or Upgrade CCS Software), Release Version (the CCS software load number), etc. You must press the ENTER or RETURN key to acknowledge selection of each (default) setting. Acceptance of these defaults will lead to installing a new release of CCS on this server.
3. After selections are complete, the software RPMs will be copied to the appropriate partition. The filesystem is now prepared to continue with server configuration and database setup.

4. The CD is ejected from the drive and the server then reboots from the hard-disk drive. The reboot will disconnect the terminal emulator's session with the server. Wait three minutes.
5. After the Avaya Services port is ready again, log in using standard Services procedures (e.g., as "craft"). You may be prompted to suppress alarm origination; press the ENTER or RETURN key to accept the default of y for yes.
6. In order to install or upgrade CCS software, you must now login as "root" (**su - root**).
7. For duplex server configurations, you can run the **ifconfig** command to verify the IP interfaces. The output of this command should display eth0 through eth3 (see Server interconnections on page 25); although not all of these interfaces are used by CCS, all should be installed correctly.
8. Both servers' RSA modules must have the latest Avaya firmware installed. From the command-line of a server, you can verify the firmware installed on its RSA module:
   a. At the root user login prompt, enter **mpcli**
   b. At the "mp" prompt, enter **logonlocal**
   c. After the SUCCESS message, enter **getvpd -mprom**
   d. If you have the required RSA firmware, the build ID on both servers of a duplex pair should be one of the following (the fourth letter will vary by firmware packet):
      - `PLET08A`
      - `PLET08B`

      If the build ID is different, then refer to Avaya's Support website and the *The Avaya RSA User's Guide*, DocID 555-245-702, for details on upgrading to the latest RSA firmware.
   e. Back at the "mp" prompt, enter **logoff**
   f. After the SUCCESS message, enter **exit**
   g. You are returned to the root user login prompt.
9. At the root user login prompt, enter the command **ccsInstaller** to run the CCS initial configuration script.
10. The ccsInstaller script prompts you for the following information:
    a. Network settings of the CCS server (select OK when you have entered these). This includes the information listed under Initial Assembly and Setup on page 29.
    b. Network settings for the ethernet port of the RSA module in this server.
    c. High Availability configuration option: n (default) for simplex or y (yes) for duplex. When installing either of the servers of a duplex pair, enter y and continue with the following steps for duplex servers. If installing a simplex server, skip these and continue with Step d.
       - When prompted to "Install High Availability Option?", type y for yes.
       - When asked "My Role in the Redundant Infrastructure?", type A (if this is the A server) or select B (the default) if this is the B server.
       - Enter the logical name referring to the duplex-server system
       - Enter the logical static IP address referring to the duplex-server system
       - Enter the physical host name and IP address of the other server in this duplex system (e.g., the name of the B server if this server is A, or vice-versa).
       - Enter the password for the Heartbeat service to use (must be the same password on both the A and B servers). Note that this password may be required for future use in troubleshooting duplex server configurations.

- Enter **username** and **password** for an administrative user of the RSA module on the A server. For an RSA module with the latest Avaya firmware, you may use the RSA user name of craft and the default password of passw0rd (with a zero, not the letter O). Note that this RSA user login information may have been changed when the module was installed or upon a full reset.
- Enter the host name and IP address of the RSA module on the B server.
- Enter **userame** and **password** for an administrative user of the RSA module on the B server. For an RSA module with the latest Avaya firmware, you may use the RSA user name of craft and the default password of passw0rd (with a zero, not the letter O). Note that this RSA user login information may have been changed when the module was installed or upon a full reset.
- If this is the first of the two servers you have configured, you will be asked, "Do you want to abort waiting for other server and make this one primary?" Do not respond. After several warning messages that the other server is not responding, a default interval for waiting will expire, and the ccsInstaller script will continue.
- You should see several messages regarding redundant services (drbd, Heartbeat), each with "OK". After viewing those messages, continue with initializing the CCS database setup in Step d.

d Next, you will be prompted to enter information for initial CCS database setup (for the postgreSQL service), such as a mvss password. You should choose an mvss database password and note that this password will be required for initial database administration (Step k) or future troubleshooting. You should see several status messages regarding the database account, both before and after the following steps. After those messages, web services will restart.

e Enter y to install a Master Administrator interface (or enter n, the default, to install a Limited one) on this server. Only one server in a CCS system (typically the Edge) has a Master interface; the other (Home) servers have Limited ones. You will be prompted whether you wish to install a Master interface on this server only if you have not specified previously that this system will have the Master Administrator interface (e.g., when configuring the A server in a duplex system). NOTE: The Master web interface can add/delete users and update data on all Home or Edge servers in a domain. The Limited Administrator interface cannot update user data.

f If you answered no to installing a Master Administrator interface in the preceding step, then you must enter the IP address of the server in your CCS system which runs the Master Administrator interface. On duplex servers, this is the logical IP address of the set. When configuring a Home server without a Master Administrator interface, enter the IP address of the Edge server that is running the Master interface in your CCS system.

g Whether you want to start CCS services now. For either server A or B of a duplex-server configuration, answer n (for no); for a simplex server, answer y (for yes) and go to Step 2 of Verify the Avaya server software installation.

For a duplex server, answer no and repeat the preceding Step 1 through Step 10 to configure the B server. After configuring B, do not start CCS services on this server either; now both of the duplex servers, A and B, will be out-of-service. Finally, continue with Step 1 of Verify the Avaya server software installation to test and bring into service each one of the duplex servers.

For a simplex server, answer yes and go to Step 2, below, to verify the software installed on the server. When the CCS-related services start successfully, you should see a series of "[OK]" messages.

Verify the Avaya server software installation - After the Avaya Services port is ready again, log in using standard Services procedures (e.g., as "admin" or "craft").

1. For a duplex-server configuration, verify each one of the two servers, in turn, as follows:
   a. 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/passed. If any tests fail unexpectedly, verify and repair the condition, as needed. (Note that you may expect that the tests checking the DNS configuration will fail if DNS has not been configured on your network.)
   b. Back at the root prompt on the B server, enter **in-service**
   c. Verify the B server's status is "In service" by executing the command **server**
   d. Repeat Step a through Step c for the A server in the duplex system.
   e. Now, reboot the A server by executing the command **reboot**
   f. Wait about five minutes for the CCS 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 CCS-related applications. After initialization is complete on this server, the results of the command should report "UP").
   g. Confirm the server is "Active" by executing the command **server**
   h. Repeat Step e through Step g to reboot the B server in the duplex system. 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" (note these server modes may be interchanged by executing the **takeover** command on the Backup server to make it the Primary).
2. For a simplex server, verify Avaya's SIP server software is running by executing the command "statapp" and then viewing the status of the applications monitored by the watchd daemon:
   a. SipServer
   b. TraceLogger
   c. Watchdog.

   NOTE:
   If the SipServer process is not listed and running on your simplex CCS host, then contact your Avaya representative.
3. You must schedule and then verify a daily CCS database housekeeping activity.
   a. Start a server telnet session, if needed, and login as "root" (**su - root**)
   b. Enter **crontab /usr/impress/sip-server/etc/vacuum-cc-db-crontab.conf**
   c. To verify the job you just submitted, enter **crontab -l** to list the jobs
   d. Enter **exit** and log off.
4. Before beginning Initial Server Administration on page 34 of this document, you should re-enable the RSA loader watchdog if you disabled it in Step 2. Refer to "Configuring the maintenance adapter" in Chapter 2 of *Installing and Configuring the Avaya S8500 Media Server*, Doc ID 03-300143, for detailed procedures for enabling the RSA loader watchdog.

Initial Server Administration

1. After the ccsInstaller script is finished and you have verified that the server(s) are running CCS, then ensure that the USB modem is connected correctly to the USB port on the x305.
2. The USB modem provides access to the Avaya Converged Communications Server to perform basic administration required to configure it for use. Once the USB modem on the x305 server has been installed and configured, you may dial into it over Point-to-Point Protocol (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 connect2 tool.
   b. Execute connect2, 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 craft -c craftpassword -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 which 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 Address field: "http://hostname/", where "hostname" is the network 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, "admin01" 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 the link to "Launch Administration Web Interface." You will receive a warning about License Error Mode; you may ignore it until after completing the Server License Installation on page 36.
   e. Select the "Setup" link to display the first of the Setup screens on page 46. Select each link on the ***Setup*** screen, in turn, to complete the initial server administration screens.
   f. From ***Setup***, select the "Setup Domain" link. The Edit System Properties screen on page 49 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 host name of the server on which you intend to enable the WebLM service for this CCS 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 duplex-server configurations, this is the logical IP address of the duplex system.
   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 97, and after confirming that this process has stopped, then select the "Start" link.) Select "Continue"
   i. From ***Setup***, select the "Setup Hosts" link. The first server you set up must be an Edge (or single Home/Edge) server. Then, if applicable, you can set up any other Home servers.

j On the Add Host screen on page 51, 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 -- A 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 a 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 was set during installation.

l Since only Home proxies must designate an Edge parent, accept the default "Parent:" of none if you are setting up an Edge or Home/Edge server.

m By default, all Listen Protocols and one Link Protocol (TLS, for CCS-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 4602 SIP telephone, or you're connecting to a SIP service provider, then you will probably check all three Listen protocols; if you're using only the IM client in IP Softphone R5 within your enterprise, then the TLS Listen Protocol is sufficient.

n (Optional) When a SIP client tries to register with this host, by default the minimum-duration registration which will be accepted is 5 minutes. If you wish to change this value, enter a new, whole integer, 1-999, in the "Minimum Registration (minutes)" field. You may accept or change the defaults for the following fields: Presence Access Policy (Default), Minimum Registration (minutes), Outbound Routing Allowed From, Outbound Proxy, Outbound Port, Outbound Transport, and Outbound Direct Domains.

o Select "Add" and then select "Continue" on the confirmation screen.

p If you just added the Edge server, then you must repeat the steps needed to add at least one Home server. (If you added a Home/Edge server, you may not add any others.) 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.

q (Optional) After you have added at least one Home server (or exactly one Home/Edge server), you may then 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 54 or the Add Media Server screen on page 56. (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

1. To obtain licenses for your Avaya CCS system, you must perform the following:
   a. Ensure that the WebLM application is installed on a Converged Communications Server. Typically, WebLM will be enabled on the Edge server (or a single, combined Home/Edge server). Then each Home server is administered to reference that WebLM application server for license verification.
   b. Ensure that you have the MAC address of the eth0 interface for the server on which you will enable the WebLM application. Note that, for RFA purposes, a duplex-server configuration is licensed as one, logical CCS system; a simplex-server configuration is licensed using its physical address.
   c. Utilize your established RFA web procedures for obtaining licenses for Avaya server(s). Note that you will need the MAC address you verified in Step b. Go to the RFA website (at http://rfa.avaya.com) and download the license file where it can be uploaded later on, typically to a location on the PC to be used by authorized services personnel.
2. After completing any remaining "Setup" screens in Initial Server Administration, you must upload and install the server license file you obtained through RFA in Step 1. You must logon and select the link to "Launch Maintenance Web Interface." From the list of available Security screens on page 180, select the link to view the WebLM Software screen on page 189.
3. Select "Enable WebLM."
4. From the list of available Security screens on page 180, select the link to view the WebLM License Admin screen on page 190.
5. Select the "Access WebLM" link. A WebLM application screen will be displayed.
6. From the WebLM screen, select "License Administration" and then enter the WebLM default administrative password of "password" (lower case, without the quote marks). Note that you can change this default.
7. Select "Browse" and navigate to the location where you saved the license file on your PC or laptop in Step 1, and then "Install license."
8. Finally, the newly uploaded license must be "acquired" by the server. If the WebLM application is running, the proxy server attempts to obtain a valid license from it every 5 minutes until either it is successful, or until the "no-license error mode" countdown time limit (typically 10 days) expires.

Tip:

If you need a server to acquire or re-acquire a license *immediately* (e.g., to quickly update the number of Home server seats you are allowed), you may restart an Avaya proxy server manually. Select the Proxy Server's "Stop" link from the Services Administration screen on page 97, and after confirming that this process has stopped, then select the "Start" link.

Communication Manager and Endpoints

1. After initial setup is complete on Avaya Converged Communications Server(s), you should use the established procedures (published in the *Administrator's Guide for Avaya Communication Manager* document) to setup the media server for use with SIP. These steps include adding users of SIP telephones and Avaya IP Softphones, adding extensions for each user, and updating proxy route patterns, as appropriate.

   Tip:

   A SIP-enabled station, such as the Avaya 4602, should be administered in Communication Manager 2.1.1 or later as an Off-Premises Station (OPS). See the *Avaya Extension to Cellular and OPS Installation and Administration Guide*, Issue 6 or later.

2. The steps that are different for SIP from the established media server setup are detailed in *SIP Support in Avaya Communication Manager*, DocID 555-245-206. These steps include entries for Signaling Group and Trunk Group setup that are specific to SIP. After you've completed setup in Communication Manager, perform a "Save Translations" to save changes.
3. After setting up Avaya IP Softphone users in Communication Manager, 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 IP Softphone application for more information. You also may wish to verify that these softphones can register with the Converged Communications Server(s), and then can send and receive instant messages, update their client buddy lists, etc.
4. After setting up SIP telephones in Communication Manager, ensure that each has the appropriate version of firmware supporting SIP. Note that the Avaya 4602 SIP phone ***requires*** that you enter a domain name on its SIP Settings page. You may wish to make and receive test calls, too.

   NOTE:

   For application notes on which third-party SIP endpoints are supported, go to the website: http://www1.avaya.com/enterprise/resourcelibrary/applicationnotes/ and then select the link for Network Infrastructure under "DevConnect Product Integration."

Upgrading an Existing Server

This section details the tasks involved in upgrading an Avaya server which is running CCS software to a newer version of software. See Configuring a New Server on page 29 to install a new server.

Types of Upgrades

For this release of CCS, there are two distinct types of server upgrades:

- **CCS Release 2.0.x to CCS Release 2.1 software.**

  User data created on the exsting server should be exported to a file and downloaded. Then the server boots from the Avaya CCS software CD and is prepared to receive the upgrade. After files have been copied and the server rebooted, you must run the ccsInstaller script as root. After a new database is created and initialized, the file of user data you saved can be uploaded and imported. Go to Before Beginning a 2.0.1 Upgrade on page 39 to upgrade CCS from release 2.0.1.

  CCS Release 2.1 to a later 2.1.x release or build.

  This should be performed using the Install New Software Wizard Steps/Pages on page 156. This process is similar to upgrading Avaya Communication Manager on Avaya S8500 Media Servers, and therefore should have no impact on service. After using the Backup Now screen on page 167, you install upgraded software in its own hard-drive partition, the server reboots using this partition, and after verifying server operation, you use the Make Upgrade Permanent screen on page 162 to make the software upgrade permanent. Then you can use the View/Restore Data screen on page 176 to restore your data backup. See below.

Additional notes when upgrading a duplex server running CCS 2.1.x

Only in the case of upgrading 2.1.x software on a duplex server, upgrade the software on the Standby (B) server first. If this is an upgrade of release 2.0.1 on a non-duplex server to a new, release 2.1 duplex-server system, you must follow the instructions for Configuring a New Server on page 29.

a When upgrading from a 2.1.x software version to a later version in a duplex-server configuration, you should log on to the Maintenance Web Interface on the Standby (or secondary, B) server and use the Status Summary screen on page 144 to verify that the server is in standby mode.

b Select "Busy-out Server" and then the "Busy-out" button. Use the Status Summary screen on page 144 to verify that the server is "out-of-service".

c Follow the Install New Software Wizard Steps/Pages on page 156 to upgrade server software. The server will reboot at the end of the upgrade process.

d Use the Make Upgrade Permanent screen on page 162 to make the software upgrade permanent. Use the Boot Partition screen on page 164 to verify that the new software version is loaded in both the "Active Partition" and the "Boot Partition".

e Put the server back in standby mode. Select "Release Server" and then the "Release" button. Use the Status Summary screen on page 144 to verify that the server is in Standby mode.

f Make the upgraded server the new Active (or primary, A) server. Select "Interchange Servers" and then the "Interchange" button. Use the Status Summary screen on page 144 to verify that the server now is in Active mode.

g Select "Exit" to close the session with this server. Logon to the Maintenance Web Interface on the other server of the duplex pair and repeat Step a through Step f to upgrade that server as well.

Before Beginning a 2.0.1 Upgrade

See Initial Assembly and Setup on page 29 for details on obtaining setup information about your server, and ensuring it is properly connected to your IP network. Then read ***all*** of these upgrade-related tasks.

1. In a terminal window, log in to Linux as "root"
2. Stop running the existing version of the server software by executing the "stop -a" command.
3. On the Export/Import screen on page 99, perform the following functions to preserve user data:
   - **a** Use the Export Database function to create a file containing the user data on your server. This file is named "mvss_admin.xml" and is written into the /tmp directory on the server.
   - **b** Use the Download Database function to save (or transfer manually using FTP) the newly exported file to your PC or laptop's local disk (or to a safe location on your network) for safekeeping during the upgrade. You can use the Upload Database and Import Database functions to retrieve this user data after the server has been upgraded.

Upgrading 2.0.1 Server Software

To upgrade a Converged Communications Server, Avaya's SIP proxy and instant-messaging server, the following tasks must be performed locally (usually by an Avaya or BusinessPartner installer):

1. If you have not done so already, stop running the existing Avaya server software by executing the "stop -a" command in a telnet window.
2. Continue with Step 1 through Step 10 for Installation of Server Software on page 30. After completing these steps, continue with the following.

Preserving Existing User Data

1. On the Export/Import screen on page 99, perform the following functions to preserve user data:
   - **a** Locate the file of existing user data you saved in Step 3 on your PC or laptop's local disk (or network location).
   - **b** Logon to the Administration Web Interface and use Upload Database on page 101 to retrieve the file (or transfer it manually to the /tmp directory on CCS using FTP).
   - **c** Use the Import Database function to retrieve this user data after the server software has been upgraded and the mvss database reinitilized on CCS.

     NOTE:
     All CCS hosts should be set up and configured with the same IP addresses as before the software upgrades, or this database import and synchronization will not be successful.

   - **d** Select the link for "Force All" to synchronize all CCS host database information.

     NOTE:
     The file contains user contact database information, including Media Server extensions. Server configuration data is not preserved.

Administering and Licensing Server

1 Continue with the following steps, which are the same as for configuring new servers:

- **a** Perform Step 3 and Step 4 of Verify the Avaya server software installation on page 33
- **b** Then proceed from Step 3 with Initial Server Administration on page 34
- **c** Continue from Step 1 through Step 8 for Server License Installation on page 36.

3 Administration Web Interface

List of Screens

The following screens are used to administer a Converged Communications Server. (Note that many of these screens only are applicable to the server running the Master interface, typically the CCS set up as an Edge or as a combined Home/Edge proxy; the administrative capabilities of Home servers typically are limited to a subset of Services and Export/Import Tasks.)

Top

At the top-most level of the master administrative interface are the following:

- ***Logon screen on page 44***
- ***Choose Interface screen on page 45***

  Select the link to "Launch Administration Web Interface" and the choices which follow appear.

After doing these initial logistical tasks, you should continue completing the screens linked from "Setup."

Setup

The names of the screens (and of the links to them) from the ***Setup screen on page 46*** are as follows:

- ***Edit System Properties screen*** on page 49 (Setup Domain)
- ***Add Host screen*** on page 51 (Setup Hosts)
- ***Edit Default User Profile screen*** on page 54 (Setup Default User Profile) -- completing any or all of the field entries on this screen is optional, but recommended if many users share characteristics. Any fields with blank entries will default to blank entries in the profiles of new users as they are added.
- ***Add Media Server screen*** on page 56 (Setup Media Servers) -- required for SIP interoperability with the extensions/users on a media server running Avaya Communication Manager.

Users

The names of the screens (and of the links to them) from the ***User Administration screen on page 58*** are as follows:

- ***List Users screen on page 60*** (List)
  - — ***Edit User Profile screen on page 69*** (Profile)
  - — ***Edit User Handles screen on page 71*** (Handles)
  - — ***List Media Server Extensions screen on page 78*** (Extensions)
- ***Add User screen on page 62*** (Add)
- ***Search Users screen on page 65*** (Search)

- ***Edit User Profile screen on page 69*** (Edit)
- Delete User (Delete)
- Change User Password (Password)
- ***Select User screen on page 67*** (Update Password, Delete User or Edit User Profile)
- ***Edit Default User Profile screen*** on page 54 (Default Profile)
- ***Registered Users screen on page 74*** (View Registered Users)

Extensions

The names of the screens (and the links to them) from the ***Manage MS Extensions screen on page 76*** are as follows:

- ***List Media Server Extensions screen on page 78*** (List)
  - — Assign Free Extension (Select Free Extension)
  - — Disassociate Extension From User (Free)
- ***Add MS Extension screen on page 79*** (Add)
- ***Search MS Extension screen on page 81*** (Search)

Hosts

The names of the screens/functions to help Manage Hosts are as follows:

- ***Add Host screen*** on page 51 (Add)
- Update All Hosts (Update)
- Force All Hosts (Force All)
- ***List Hosts screen on page 82*** (List)

Media Servers

The names of the screens (and the links to them) from the ***Manage Media Servers screen*** are as follows:

- ***List Media Servers screen on page 87*** (List)
  - — ***Add Address Map screen on page 89*** (Map)
  - — ***List Address Map screen on page 91***
    - ***Edit Map Entry screen on page 93*** (Edit)
    - ***Edit Contact screen on page 95*** (Edit)
- ***Edit Media Server screen on page 88*** (Edit)
- ***Add Media Server screen*** on page 56 (Add)

Services

The name of the screen used to start/stop the processes related to Avaya's SIP proxy and instant-messaging server is as follows:

- ***Services Administration screen*** on page 97 (Services)

Export/Import

The names of the screens (and the links to them) from the ***Export/Import screen*** on page 99 are as follows:

- Export Database screen (Export)
- Download Database screen (Download)
- Import Database screen (Import)
- ***Upload Database screen on page 101*** (Upload)
- ***IM Logs screen on page 102*** (IM Logs)

Server Configuration

The names of the screens (and the links to them) from the ***Server Configuration screen on page 103*** are as follows:

- ***Edit System Properties screen*** on page 49 (System Properties)
- ***List Domain Access screen on page 105*** (Manage Domain Access)
  - — ***Add Domain Access screen on page 107*** (Add Another Entry)
- ***List Administrators screen on page 109*** (Admin Accounts)
  - — ***Add Administrator screen on page 110***
  - — ***Change Administrator Password screen on page 111***
- ***Manage Licenses screen on page 112*** (License)
- ***IM Log Settings screen*** on page 114 (IM Log Settings)

Top-Level Screens

Logon screen

Logon screen field descriptions

Logon ID

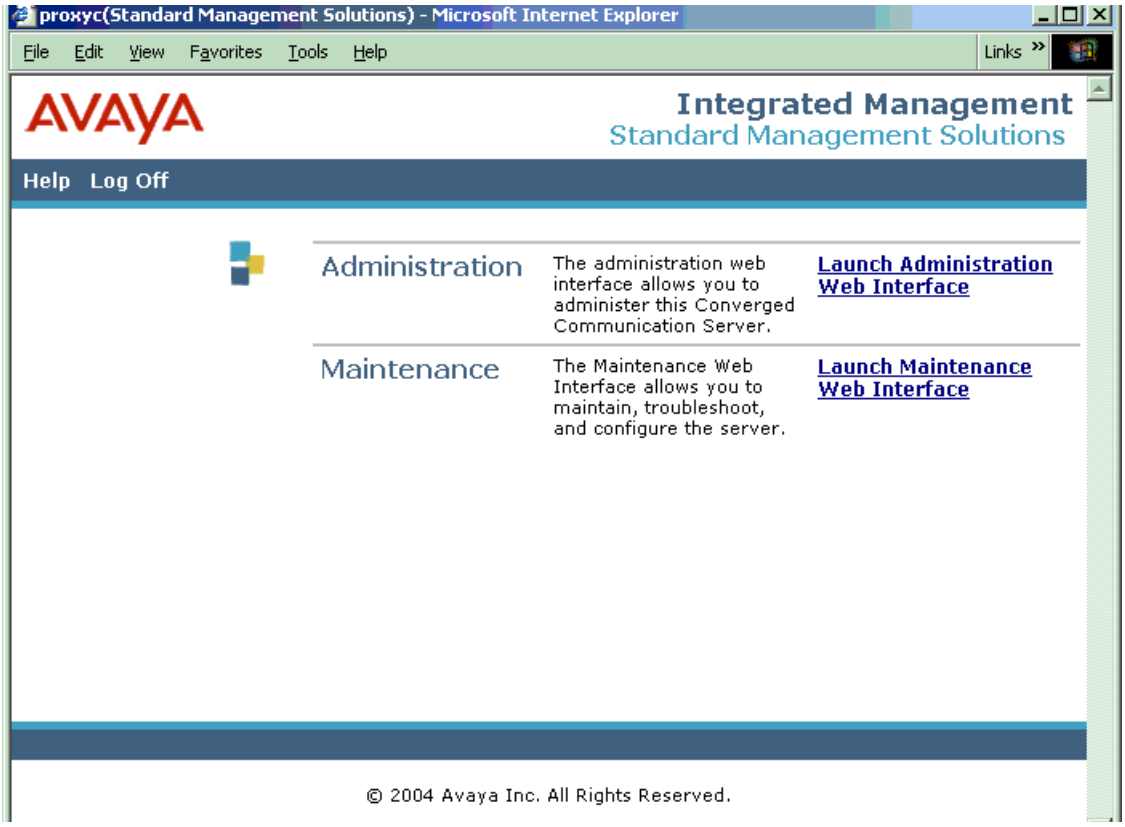
(Required) Enter the user name with which to log on to your administrative account. After you enter this and press the Return key or select "Logon", the screen will refresh with the following Password field.

Password

(Required) Enter your adminstrative 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 the Enter or Return key on your keyboard.

Choose Interface screen



Choose Interface screen field descriptions

Use the Choose Interface screen after logon to select from either the Administration Web Interface or the Maintenance Web Interface, depending on what functions you need to perform on the server.

Administration

The administration interface is used for initial server setup, user contact database changes and media server related activities. Select the link to the right to "Launch Administration Web Interface."

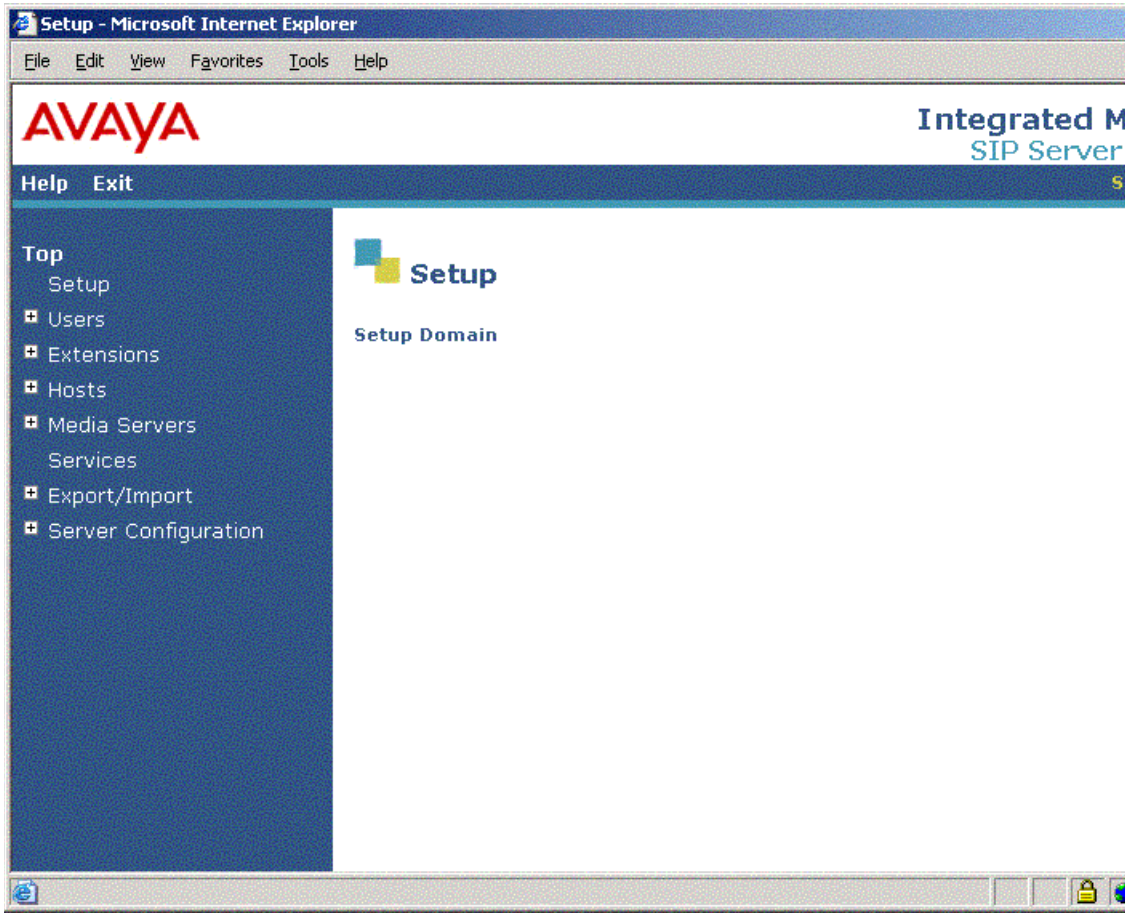
Maintenance

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

Setup screen

The Setup screen shows link(s) to the next screen(s) needed to configure the Avaya Converged Communications Server for initial use. This screen will display different choices, depending on which required tasks have been completed. The first Setup screen displayed typcially would be as follows:

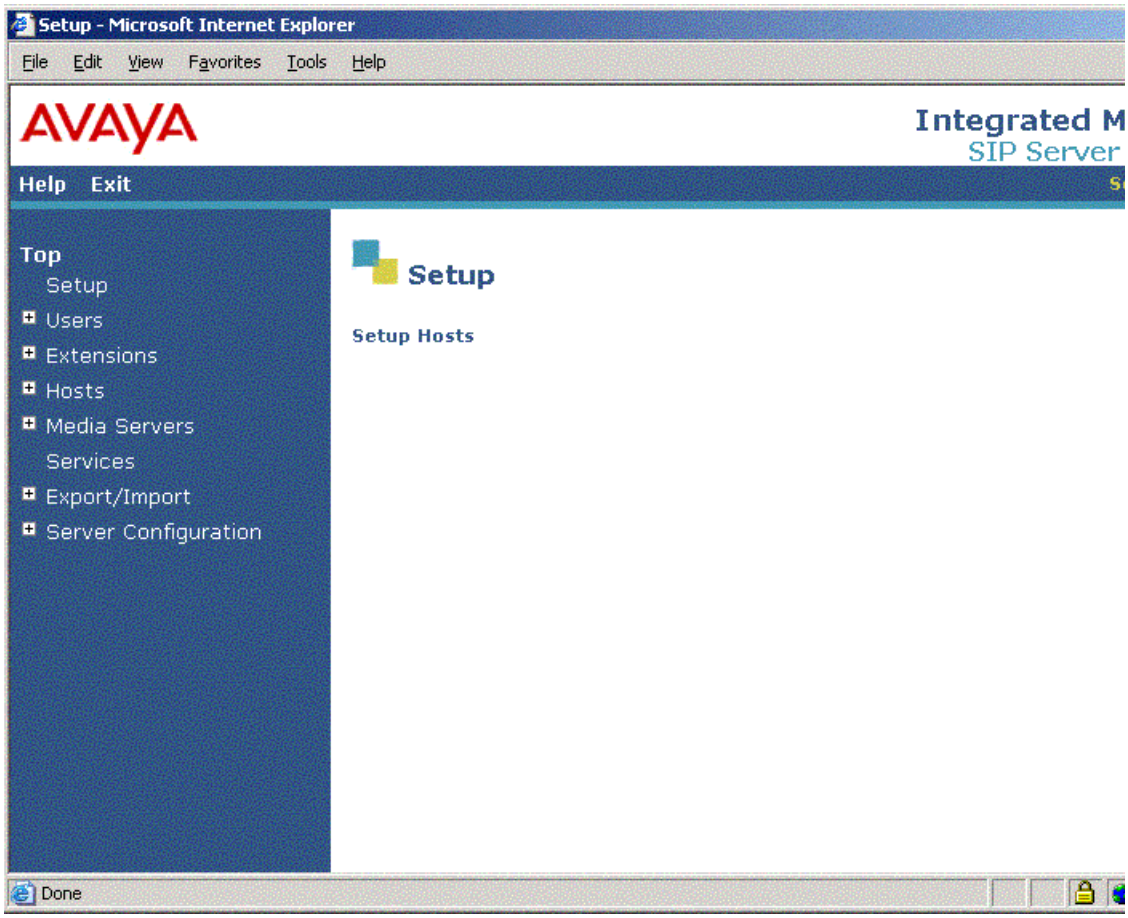


Setup screen field descriptions

Setup Domain

Select this link to go to the ***Edit System Properties screen*** on page 49. You must specify the domain to assign to this system 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 domain will be recognized system-wide. From the ***Services Administration screen*** on page 97 , select the "Stop" link for the Proxy Server, confirm that the process stopped, and then select the "Start" link.

The next Setup screen that typically appears would be as follows:

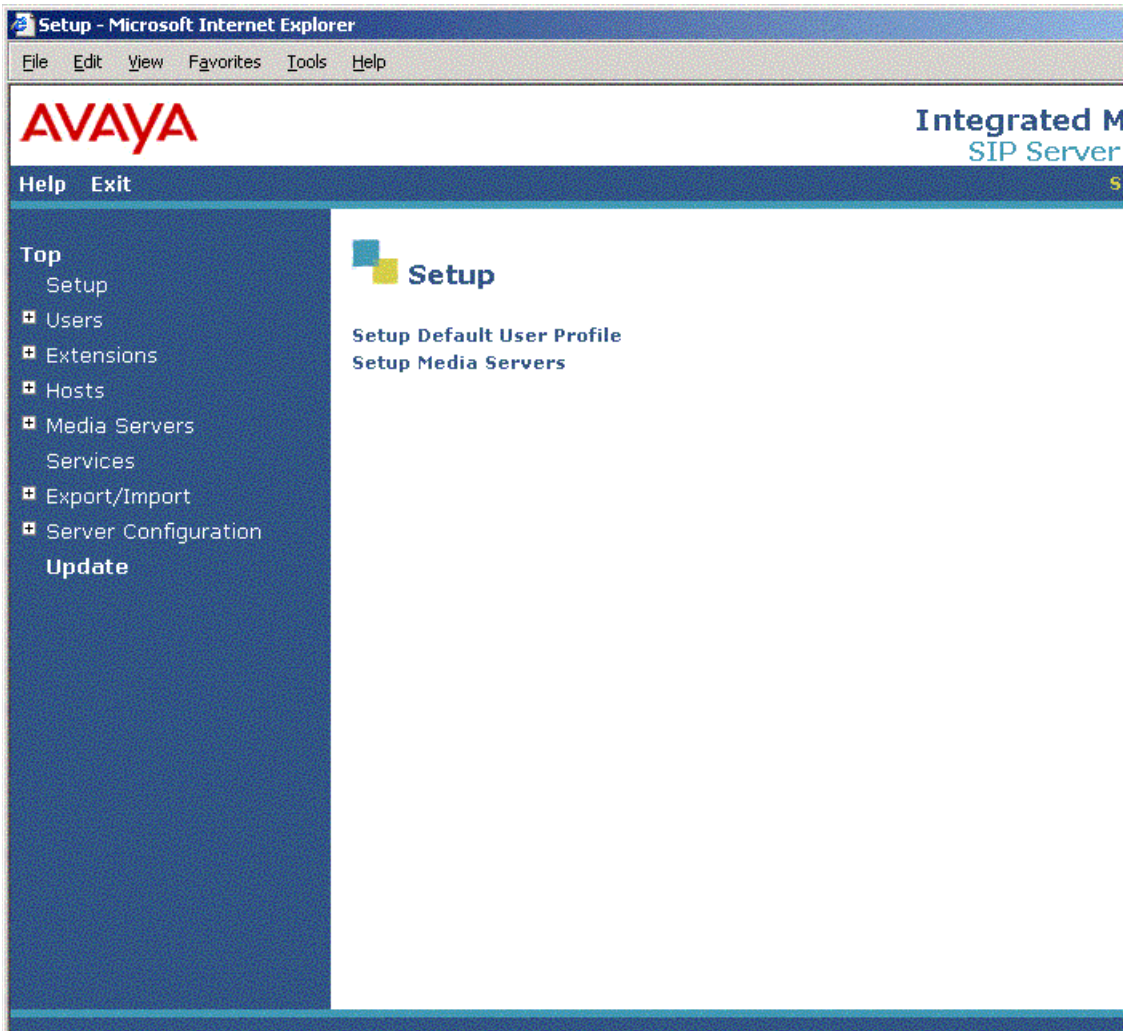


Setup Hosts

After setting up the CCS system domain, select this link to go to the ***Add Host screen*** on page 51 and create a host computer entry for this Converged Communications Server(s) in your enterprise.

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 will display two other choices. Completing these screens is optional, but is recommended before continuing with user (contact) or extension (telephone number) administration.



Setup Default User Profile

This link appears after at least one Home (or exactly one Home/Edge) server has been added via the "Setup Hosts" link. Now you may select this link to go to the ***Edit Default User Profile screen*** on page 54, or you may choose first to set up your system's media servers running Communication Manager.

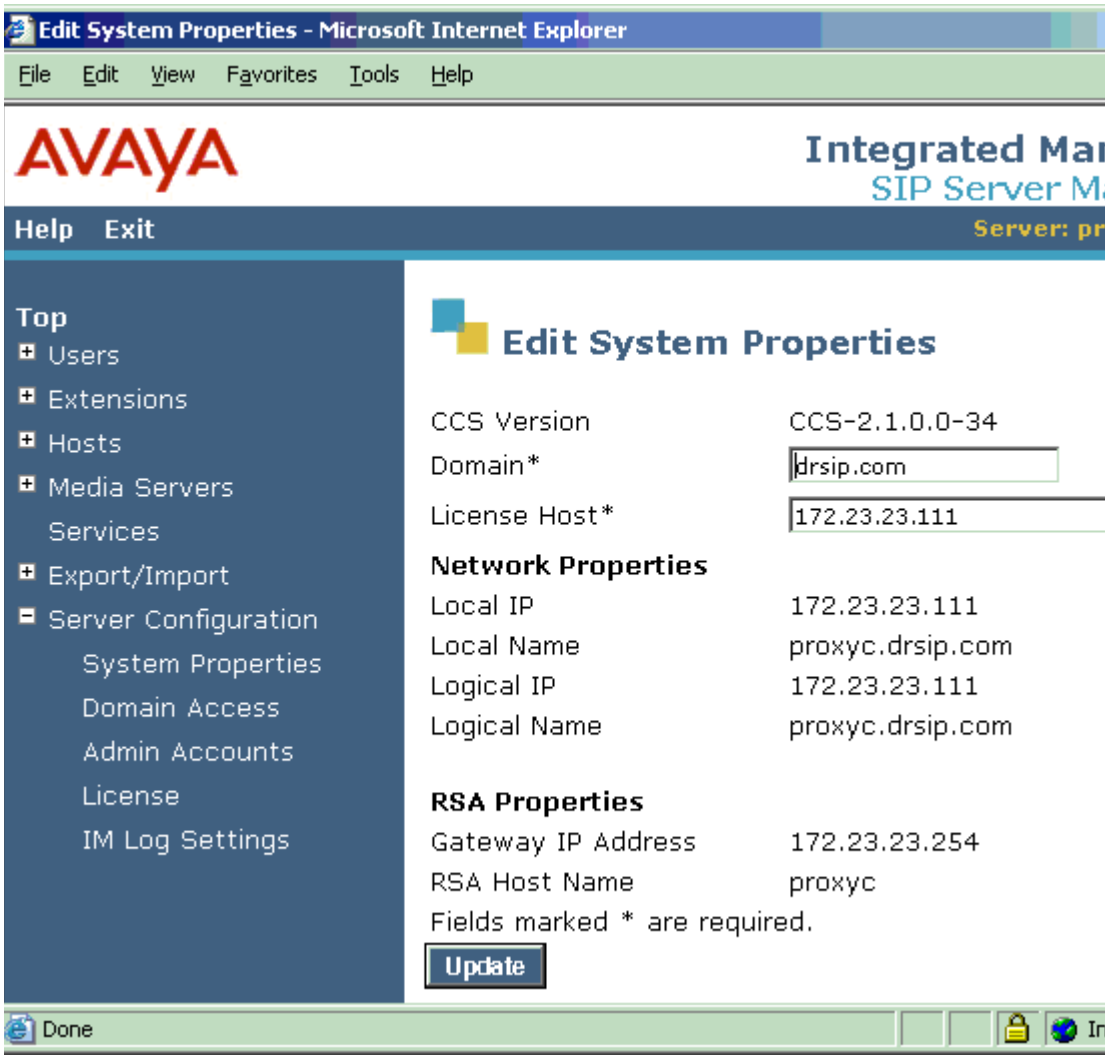
Setup Media Servers

This link appears after any type of host has been added via the "Setup Hosts" link. Select this link to go to the ***Add Media Server screen*** on page 56 and create one or more entry or entries for your network's media server(s) running Avaya Communication Manager. Media Gateways must also be up-to-date.

Tip:

Note that you may not add user information (e.g., contacts) or media server extensions (telephone numbers) to the database until these setup options have been completed.

Edit System Properties screen



Edit System Properties screen field descriptions

CCS Version

(Read Only) This field displays the major and minor release number (2.1.0.0) and the current load/build number (34) of the Avaya software that is running on this Converged Communications Server.

Domain

(Required) Enter a domain name to assign to this Converged Communications Server. For a Customer's Edge server running the Master interface, this might be "customer.com"

License Host

(Required) Enter 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.

Network Properties

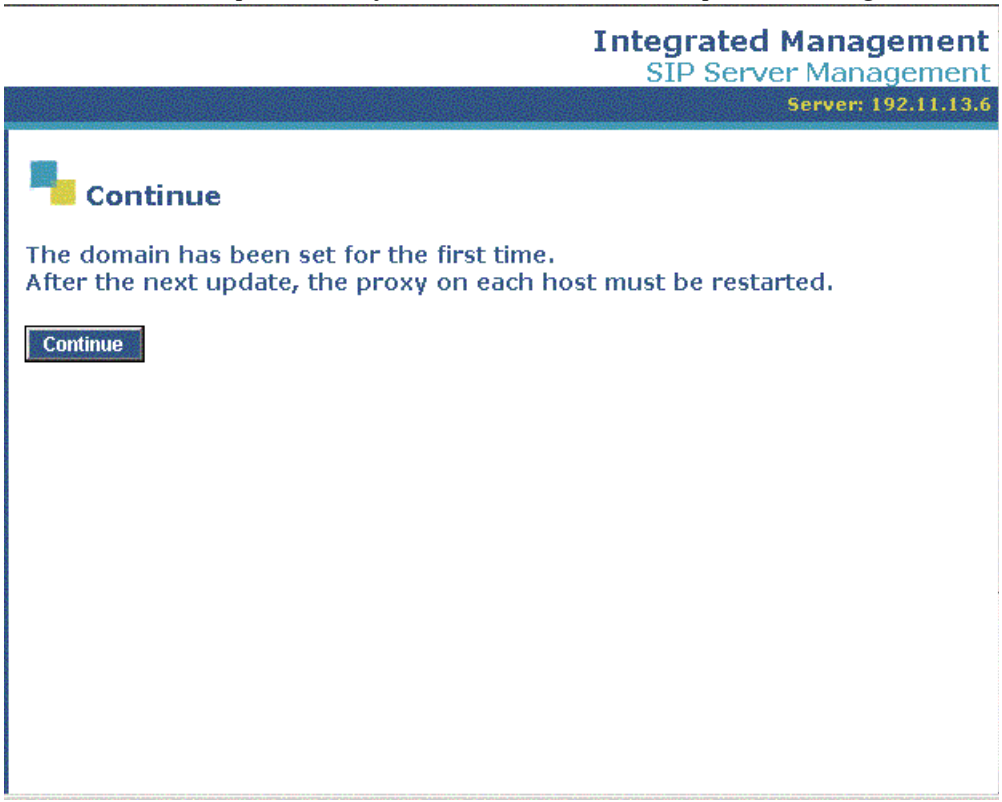
(Read Only) Lists the **Local IP** address and **Local Name** for this physical server, as well as the **Logical IP** and **Logical Name** for this CCS node. Local and Logical properties are the same for each server in a simplex configuration; on a server that is one of a duplex pair, its Local properties will differ from its Logical ones. However, the Logical properties will be the same for both of the servers of a duplex pair.

RSA Properties

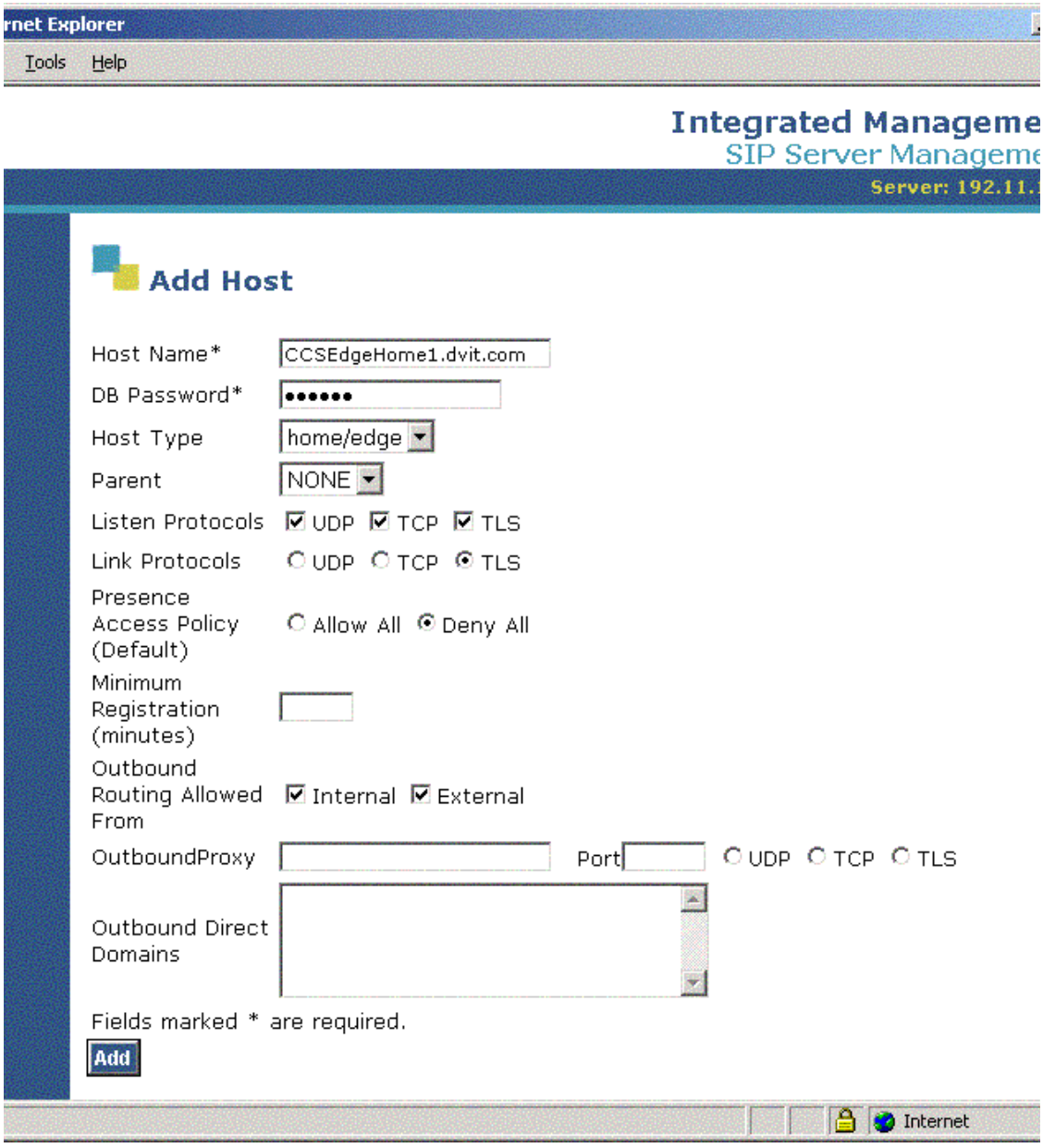
(Read Only) Lists the **Gateway IP Address** and **RSA Host Name** for the RSA module in this CCS host. Note that this information cannot be changed from within this Administration Web Interface.

Select "Update" to submit the updated information on this host. Then all the hosts should be updated.

NOTE:
Updates to system-wide properties like the domain will require that the proxy service on each SIP host computer in the system be restarted before the updates are recognized.



Add Host screen



Add Host screen field descriptions

Host Name

(Required) Enter the fully qualified domain name or IP address for this CCS host (server).

DB Password

(Required) Enter the password assigned to the database at installation, which should be at least 4 alphanumeric characters in length.

Host Type

Select one of the following from the drop-down list:

- edge -- if this will be an Edge proxy 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 handle 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

Select one of the following from the drop-down list:

- NONE -- if you selected edge or home/edge for the server's Host Type, above.
- {HOSTNAME or IP} -- if you selected home for the server's Host Type, above, and the name of the edge proxy for all your enterprise's domains is listed, then select it as Parent.

Listen Protocols

Select any or all of the three listed protocols as protocols for which the server should listen:

- UDP (User Datagram Protocol)
- TCP (Transport Control Protocol)
- TLS (Transport Link Security)

By default, all protocols are selected to be used by the proxy to listen to/for endpoints. Note that the protocol which is selected 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

Select exactly one of the three listed protocols to be used for purposes of linking together SIP proxy hosts (home and edge servers, for instance) in your Avaya CCS system: UDP, TCP and/or TLS (the default proxy server link protocol). You must also select the Link Protocol as a Listen Protocol, above; you may want to select additional listen protocols, but you ***may not*** select any additional protocols for linking.

Presence Access Policy (Default)

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.

Minimum Registration (minutes)

Enter a whole number of minutes, 1-999, 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 5 minutes will be used.

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 handle 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. On a Home/Edge or Edge proxy server, an entry in this field typically is not required.

Outbound Port

Enter the number of the port (1-65535) on the outbound proxy server specified above that should handle 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 Transport

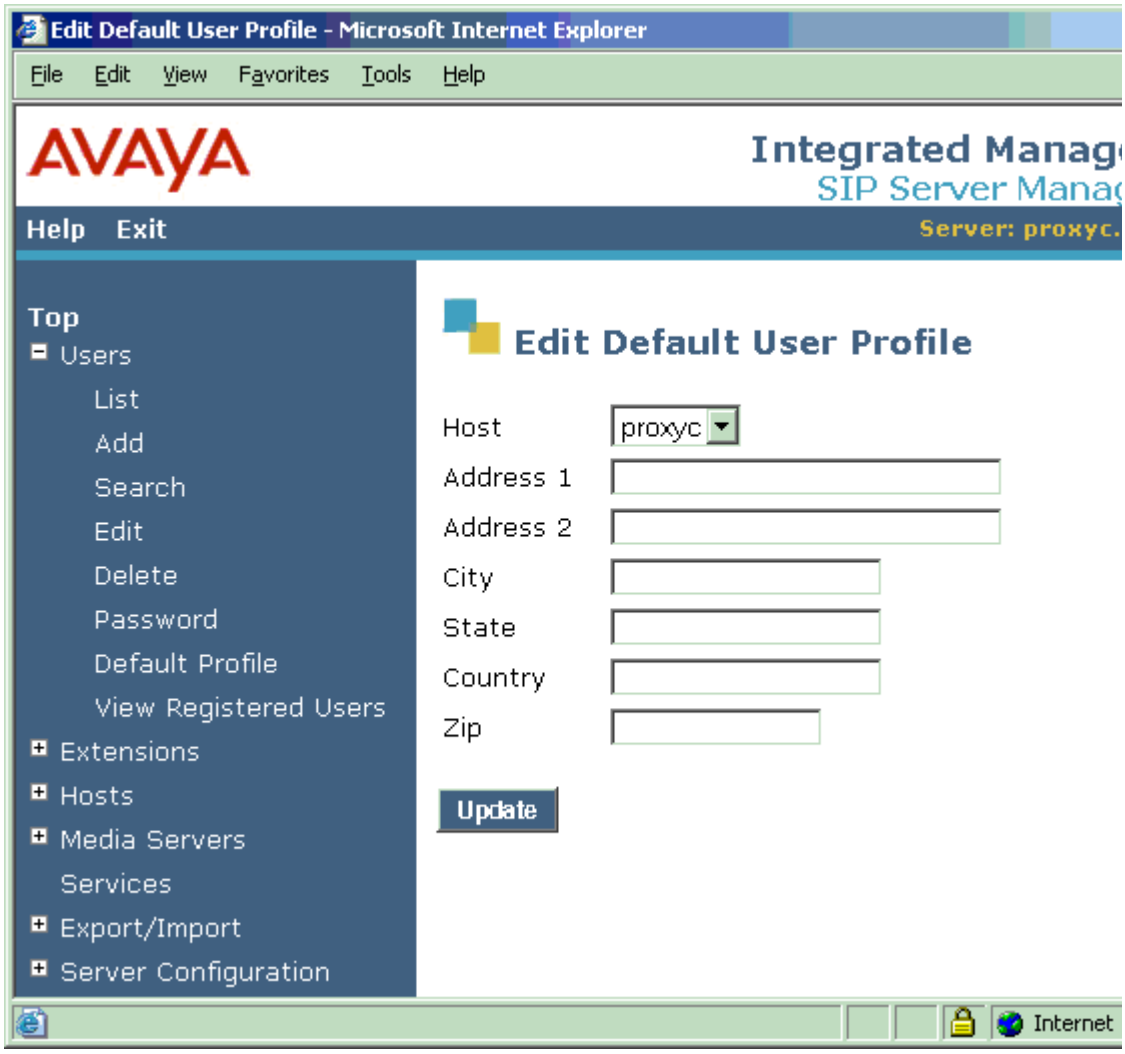
Select the transport protocol of the outbound proxy server that should handle SIP traffic bound for domains external to this server's domain. TLS is recommended if the outbound proxy supports it.

Outbound Direct Domains

List those domains for which traffic may completely bypass 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 CCS host with the properties you've entered. If you have added an Edge proxy, then selecting "Continue" at the next screen will return to the ***Add Host screen*** on page 51 until a Home proxy has also been added. If you add a combined Home/Edge proxy, then you'll return to the ***Setup screen on page 46***.

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 CCS host for whose users this location information will become the default entries. The hostname selected by default in the list is the first Home server alphabetically (or the one Home/Edge server, if applicable).

Address 1, Address 2

Enter the first line and second lines, respectively, of the default address for users served by this host. Use alphanumeric characters.

City

Enter the name of the city or town of the default address for users served by this host. You may use alphanumeric characters.

State

Enter the name of the state or province of the default address for users served by this host. You may use alphanumeric characters.

Country

Enter the name of the country of the default address for users served by this host. You may use alphanumeric characters.

Zip

Enter the number of the zip or postal code of the default address for users served by this host. You may use only numeric characters.

When you have entered the desired default location information, select "Update" to submit it on this host.

Add Media Server screen

If you are administering SIP trunking on your media server(s) running Avaya Communication Manager, then you should use this screen to add the SIP-enabled media server(s) to your CCS system.

Add Media Server screen field descriptions

Media Server Name

(Required) Enter a friendly name in alphanumeric characters referencing 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. Refer to "*Administration for Network Connectivity for Avaya Communication Manager,*" Doc ID 555-233-504.

Host

From the alphabetized drop-down list of names, select the name of the host computer connected to the media server's SIP trunking. The hostname selected by default in this list is that of the first Home server alphabetically (or the single Home/Edge server, if applicable).

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.

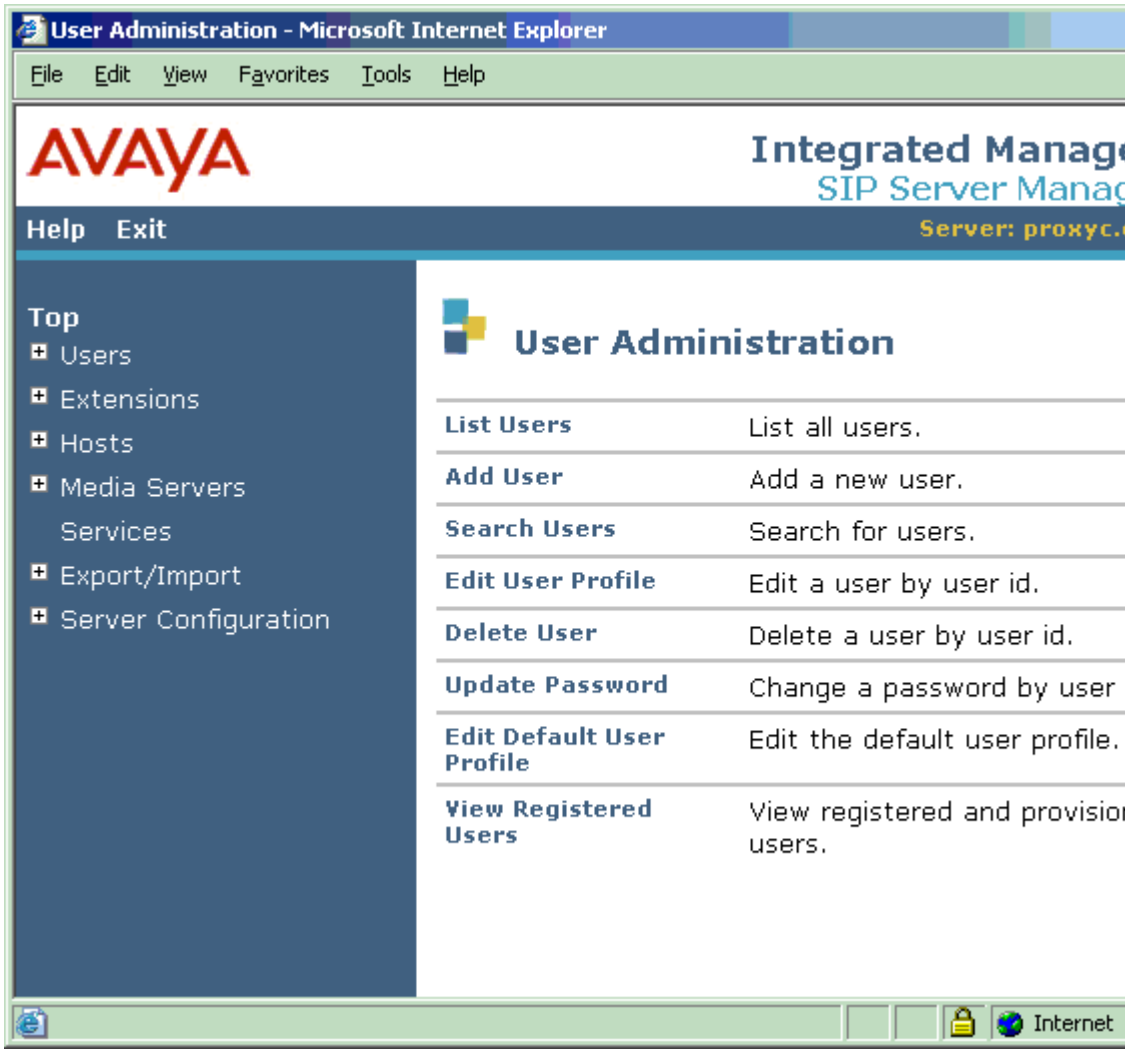
Name or IP Address

(Required) The IP address for the media server's CLAN (or processor CLAN), specified as a 32-bit address comprising 4 8-bit octets (i.e., each 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.

Select "Add" to submit the media server with the properties you've entered to this host's database.

User screens

User Administration screen



User Administration screen field descriptions

List Users

Select this link to go to the ***List Users screen on page 60*** and view all users administered in the database.

Add User

Select this link to go to the ***Add User screen on page 62*** and create a contact database entry for a new user.

Search Users

Select this link to go to the ***Search Users screen on page 65*** to use entries in the contact database as search criteria to find one or more users' profile(s).

Edit User Profile

Select this link to go to the ***Select User screen on page 67*** 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 go to the ***Select User screen on page 67*** and enter a user ID for the user whose profile you want to delete.

Update Password

Select this link to go to the ***Select User screen on page 67*** and enter a user ID for the user whose password you want to change.

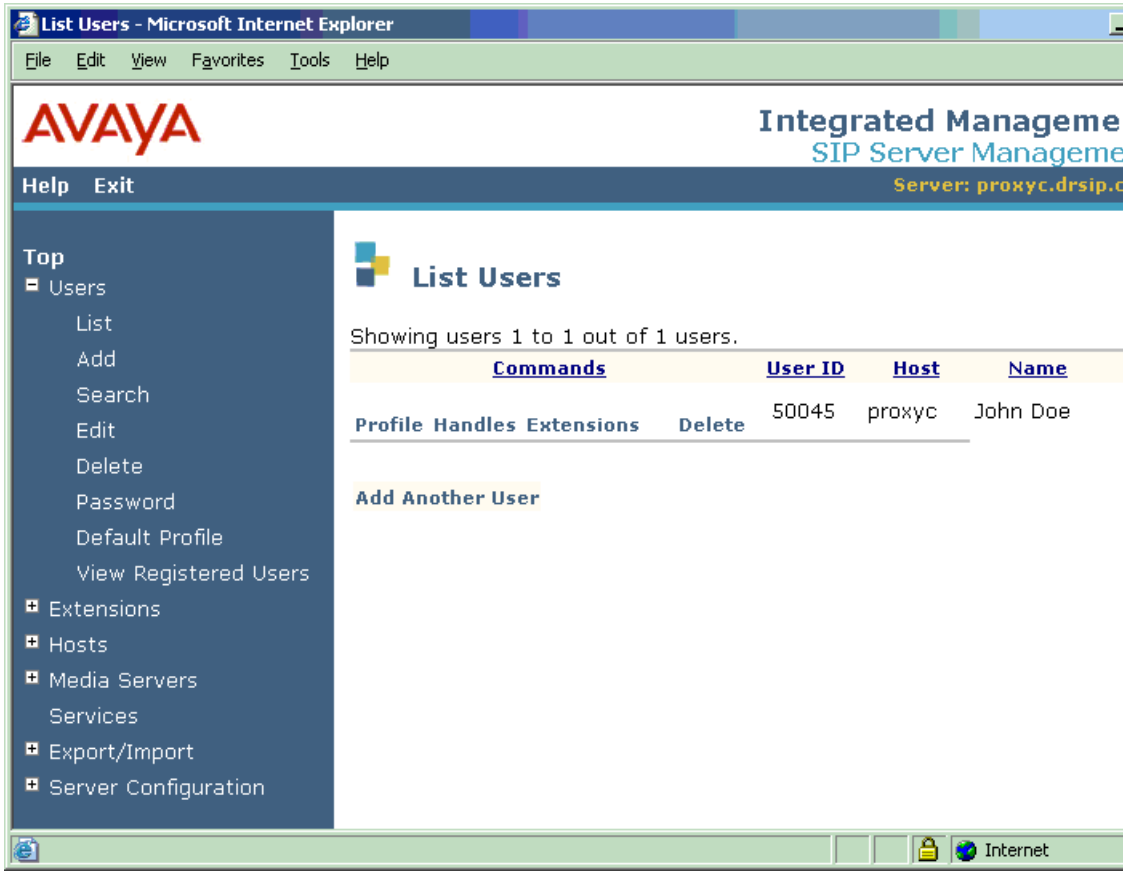
Edit Default User Profile

Select this link to go to the ***Edit Default User Profile screen*** on page 54 and modify one or more entry or entries. Note that this will modify the default values to be populated in the profiles of all new users created.

View Registered Users

Select this link to go to the ***Registered Users screen on page 74*** and view those users that have SIP clients that have registered to, or been provisioned on, this server.

List Users screen



List Users screen field descriptions

User ID

(Read Only) Lists the IDs of previously administered users in the database.

Commands

You may select any of the following links next to a User ID in the Commands field:

- Profile -- to go to the ***Edit User Profile screen on page 69*** for that user
- Handles -- to go to the ***Edit User Handles screen on page 71*** for that user
- Extensions -- to go to the ***List Media Server Extensions screen on page 78*** for that user
- Delete -- to display the ***Confirm Delete User screen on page 73*****.**

Host

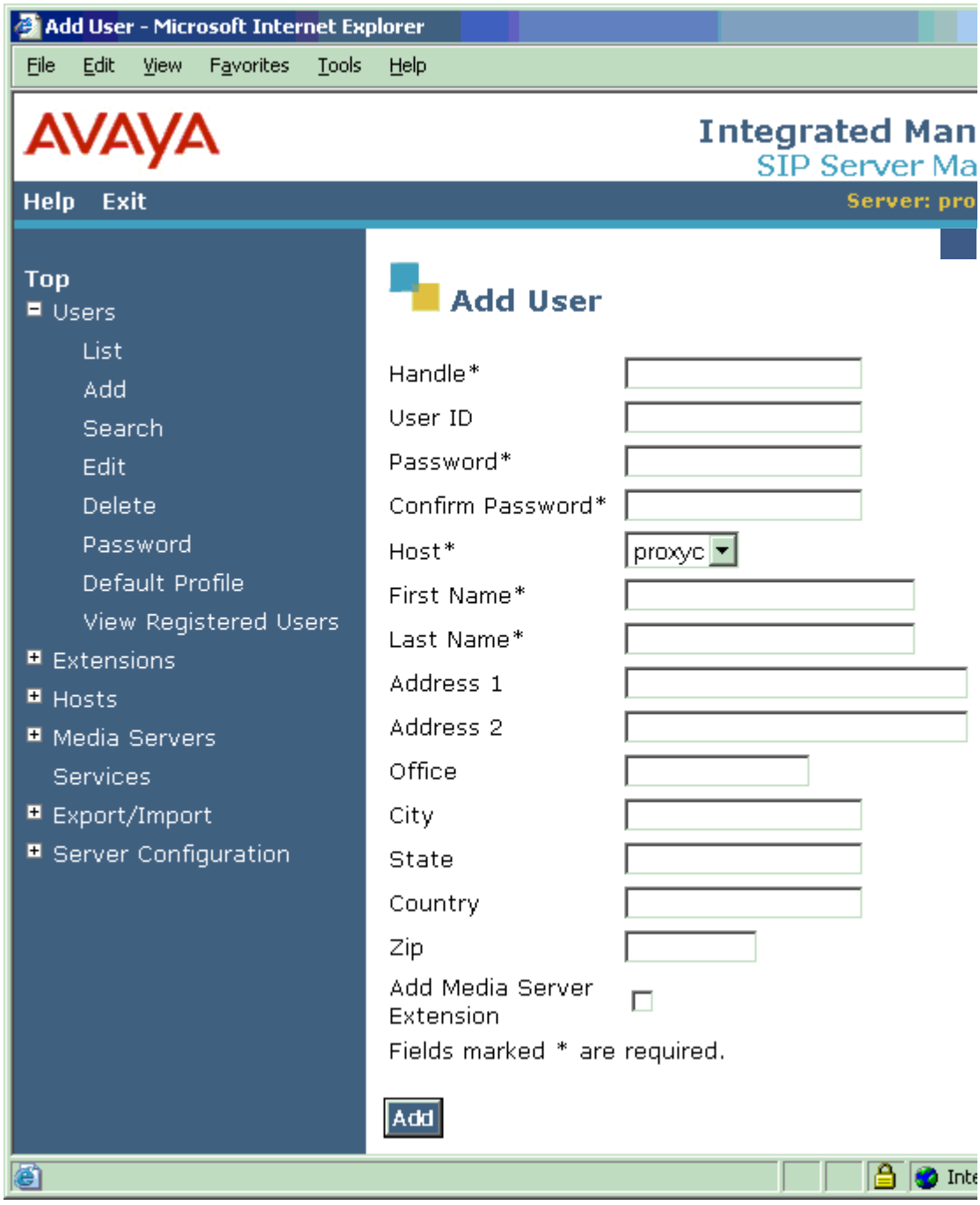
(Read Only) Displays the name of the Converged Communications Server host serving the domain for this user.

Name

(Read Only) Displays the name specified for this User ID in the database.

You may select "Add Another User" to go to the ***Add User screen on page 62***.

Add User screen



Add User screen field descriptions

Handle

(Required) Enter a "handle" name for the user of at least 3 alphanumeric characters in length. Each handle must be unique within the domain, but users may have more than one assigned to them.

User ID

(Optional) Enter an identifying name, which is at least 3 alphanumeric characters in length and is used to authenticate user clients (for example, IP Softphone to IM server). Each user has exactly one user ID. By default, it is the same as the handle, above.

Password, Confirm Password

(Required) Enter a password of at least 6 alphanumeric characters; both field entries must match exactly.

Host

(Required) From the drop-down list of names, select the host serving the domain for this user. The hostname of the current server is selected by default.

First Name

(Required) Enter the first name of the user in alphanumeric characters.

Last Name

(Required) Enter the last name of the user in alphanumeric characters.

Address 1, Address 2

Enter the first and second lines, respectively, of the user’s address in alphanumeric characters. The default is populated from the default user profile you have setup, if any.

Office

Enter the designation for the user’s office/floor, etc. 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

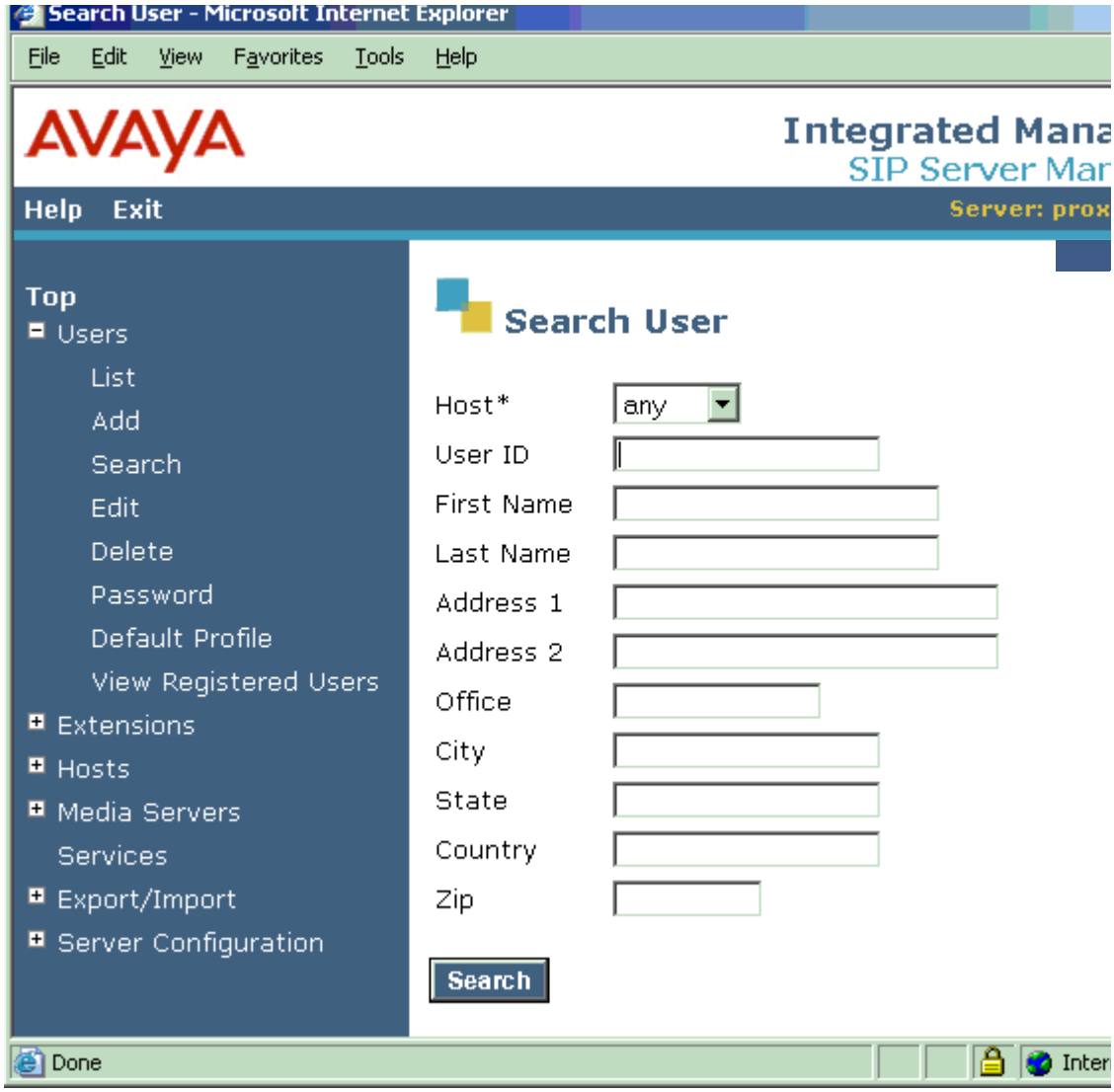
Enter the number of the zip or postal code of the user in numeric characters.

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 MS Extension screen on page 79*** 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.

After entering/updating entries, select "Add" to submit the user’s profile to the database on this host.

Search Users screen



Search Users screen field descriptions

Host

(Required) From the drop-down list of names, select the host serving the domain for the user. By default, "any" is selected, which searches all the CCS hosts you have administered for your enterprise.

User ID

If you wish to search by ID, enter a valid User ID (which is at least 3 alphanumeric characters in length).

The following fields allow for partial matches. Enter a few characters to limit the results.

First Name

If you wish to search by name, enter the first name of the user in alphanumeric characters. (No punctuation is allowed.)

Last Name

If you wish to search by name, enter the last name of the user in alphanumeric characters. (No punctuation is allowed.)

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.

Office

Enter the designation for the user's office/floor, etc. 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

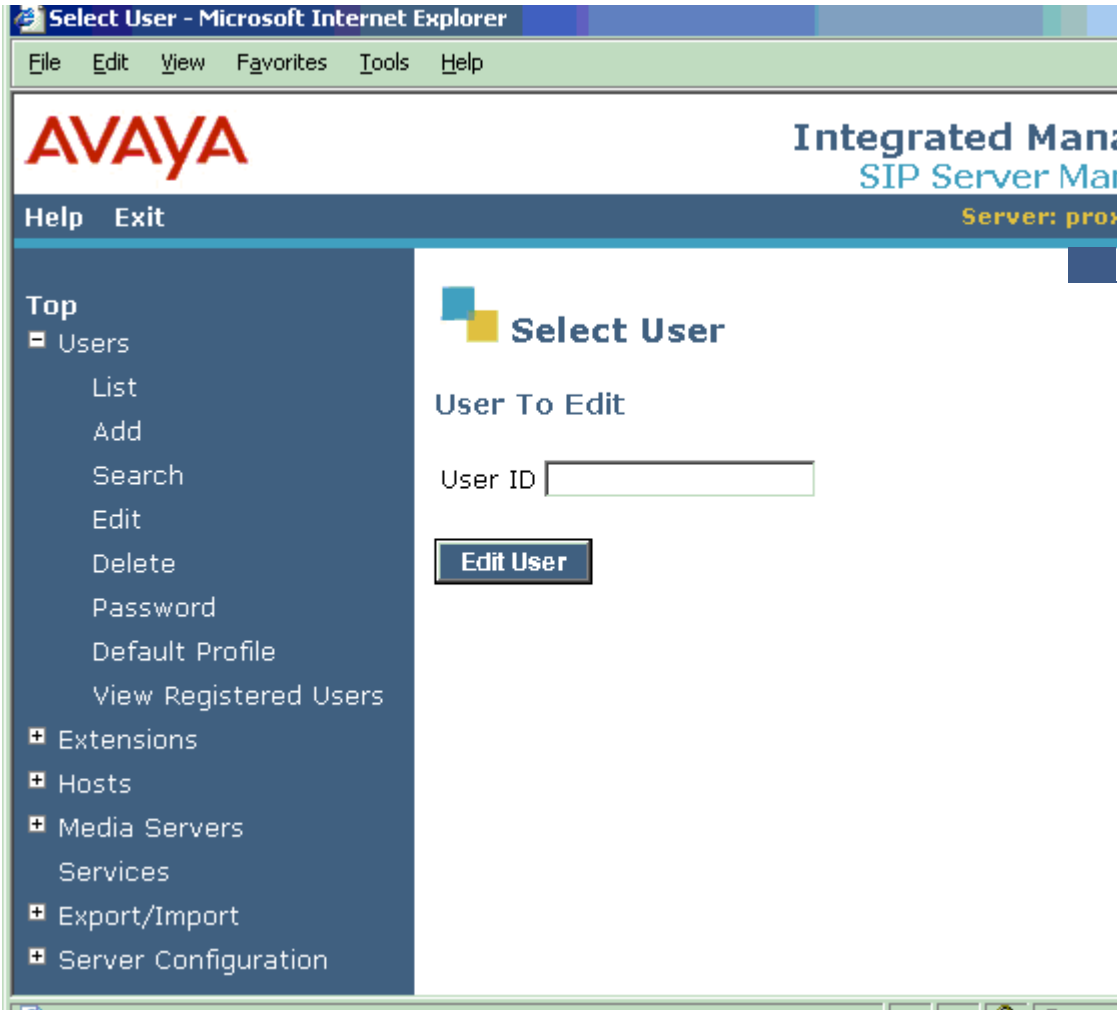
Enter the name of the country of the user's address in alphanumeric characters.

Zip

Enter the number of the zip or postal code of the user in numeric characters.

After you've entered the information on which you want to match in the database, select "Search."

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.

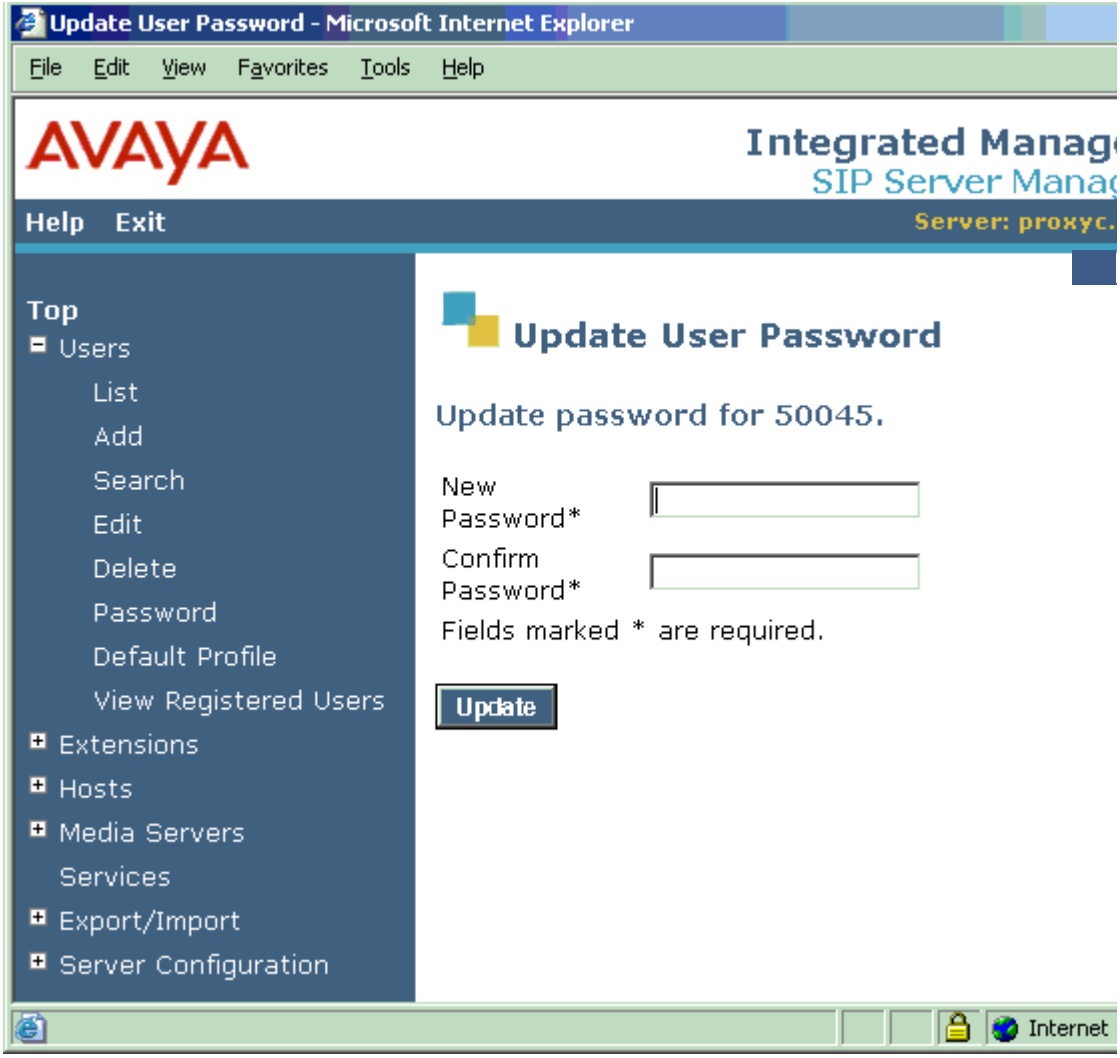
Select User screen field description

User ID

(Required) Enter a valid User ID in the database (which is at least 3 alphanumeric characters in length).

When you are ready to submit your entry, select the Edit User button.

Update Password screen



Update Password screen field descriptions

User ID

(Read Only) Shows the username of the user, which is at least 3 alphanumeric characters in length.

New Password, Confirm Password

(Required) Enter a password of at least 6 alphanumeric characters; both field entries must match exactly.

After entering and confirming the new password, select "Update" to submit it to the host's database.

Edit User Profile screen

Edit User Profile screen field descriptions

User ID

(Required) Enter an identifying name, at least 3 alphanumeric characters in length, which is used to authenticate a user's client to the CCS. Each user has but one user ID, though it need not be unique.

Password, Confirm Password

(Optional) Enter an optional password of at least 6 alphanumeric characters; any entries in these two fields must match exactly.

Host

(Read Only) Displays the CCS host (a Home or combined Home/Edge server) serving the domain for this user.

First Name

(Required) Enter the first name of the user in alphanumeric characters.

Last Name

(Required) Enter the last name of the user in alphanumeric characters.

Address 1, Address 2

Enter the first and second lines, respectively, of the user's address in alphanumeric characters. The default is populated from the default user profile you have set up, if any.

Office

Enter the designation for the user's office/floor, etc. 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.

After entering/changing entries, select "Update" to submit the user's profile to the database on this host.

Edit User Handles screen

Edit User Handles screen field descriptions

User ID

(Required) An identifying name, which is at least 3 alphanumeric characters in length and is used to authenticate a user's client to the server. Each user has but one user ID, though it need not be unique.

Host

(Read Only) Displays the proxy host (a Home or combined Home/Edge server) serving the domain for this user.

Handle

(Read Only) A "handle" (i.e., alias) name for the user of at least 3 alphanumeric characters in length. Each handle must be unique within the domain; users may have more than one assigned to them.

Contact

The associated Contact for this User ID in the database; this contact may be a fixed destination, or it may be constructed dynamically to include any of the components in the original SIP request URI. See the description of the field's syntax in Contact on page 92.

Commands

You may select any of the following links next to a Handle or next to a Contact in the Commands field:

- Edit -- to go to the ***Edit Handle screen*** for that user's Handle, or to go to the ***Edit Contact screen*** ***on page 95*** for the associated user Contact.
- Delete -- to display the ***Confirm Delete Handle screen*** for that user's Handle, or to display the ***Confirm Delete Contact screen*** for that user Contact entry.

Or you may select "Add Another Handle" to go to the ***Add Handle screen*** or "Add Another Contact" to go to the ***Add Contact screen***. You may also select "Add Handle In New Group" to go to the ***Add Group screen*** or "Delete Group" to display the ***Confirm Delete Group screen*** for that group.

After entering/changing entries, select "Update" to submit the user's information to the database.

Confirm Delete User screen

Confirm Delete User screen field descriptions

Confirm Delete

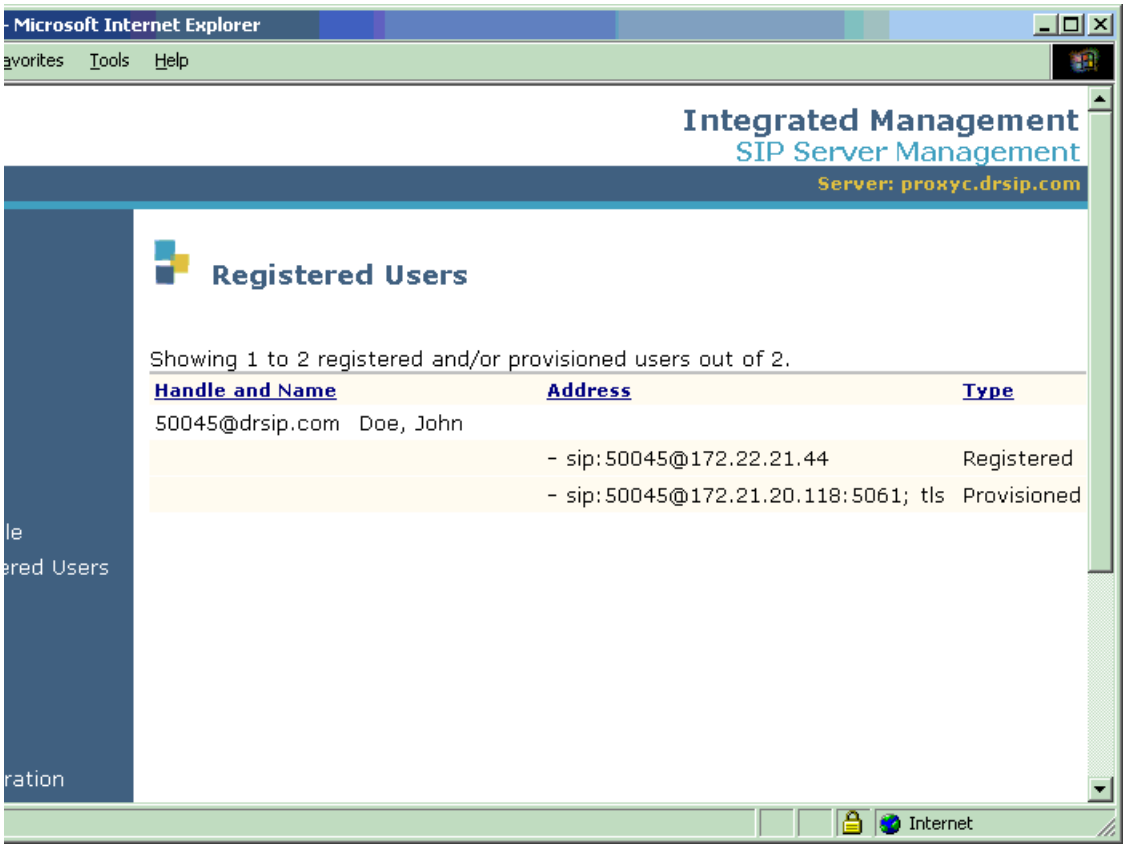
(Read Only) Informs you of which user you have selected for deletion from the database.

Delete Extensions Also

Check this box to delete the media server extensions associated with this user from the database as well; leave the box unchecked (the default) to leave the unassociated extensions free for another user to use.

Select "OK" to delete the user (and associated extensions, if applicable); select "Cancel" to ignore your original deletion selection, keeping the user and associated extensions in the database unchanged.

Registered Users screen



Registered Users screen field descriptions

Handle and Name

(Read Only) Displays both the handle and the last name, first name specified for this User ID in the database.

Address

(Read Only) Lists the SIP addresses for registered users previously administered in the database.

Type

(Read Only) Displays the type for users, either **Provisioned** (if they use an endpoint managed by Avaya Communication Manager) or **Registered** (if they have registered directly with CCS).

Media Server Extensions

Manage MS Extensions screen

Manage MS Extensions screen field descriptions

List Extension

Select this link to go to the ***List Extension*** screen and view the administered telephone extensions.

Add Extension

Select this link to go to the ***Add Extension*** screen and create an extension 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:

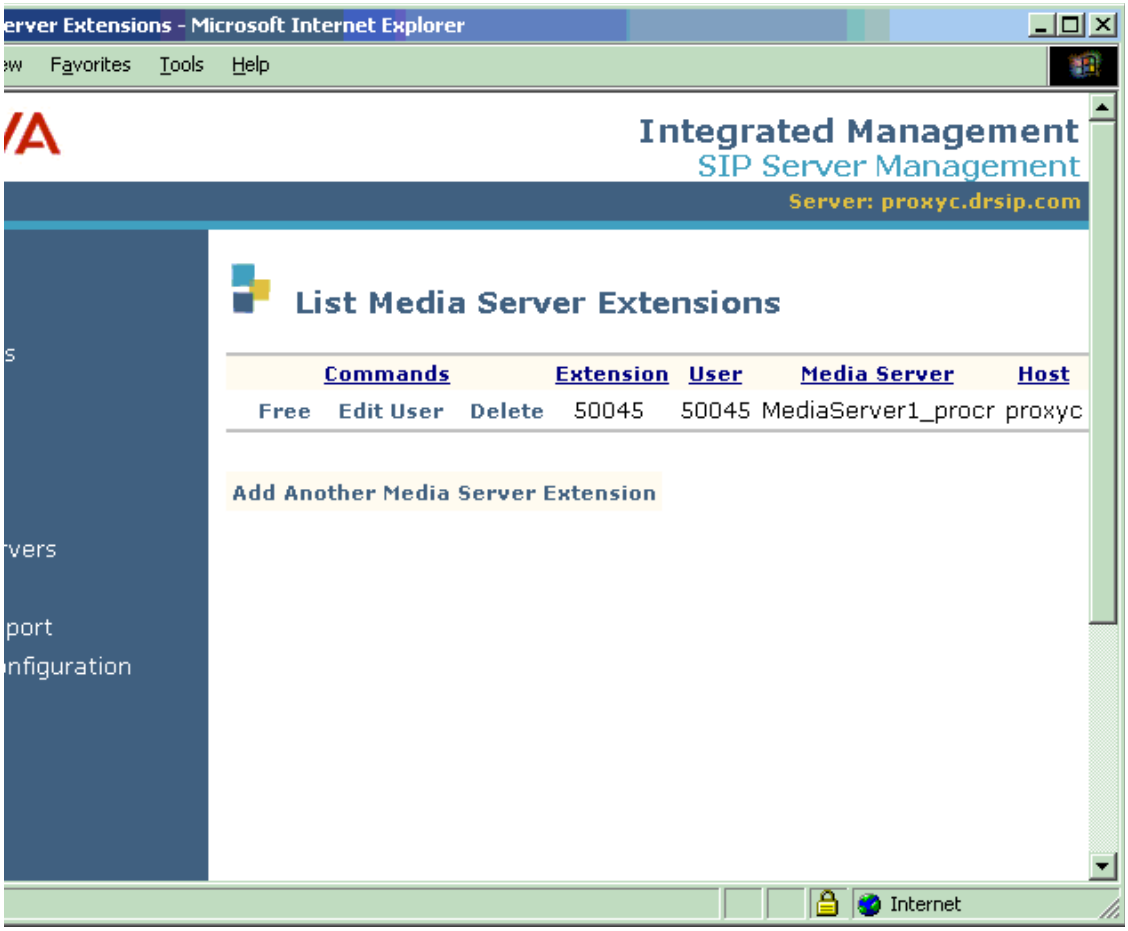
Avaya highly recommends the following general user administration guidelines:

- Each SIP-enabled endpoint is administered as an Off-Premises Station (OPS) in Avaya Communication Manager.
- Extensions for all users of Avaya IP Softphone clients set up in Communication Manager must be added to CCS explicitly and associated with their User IDs. The Administration Without Hardware (AWOH) extension administered on the media server must match the extension administered on CCS. This is so that the users' SIP URIs (for example, 1234567890@mediaserver.domain.com) may be used as their handles 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 90.

Search Extensions

Select this link to go to the ***Search MS Extension screen on page 81*** and find an extension by media server or prefix.

List Media Server Extensions screen



List Media Server Extensions screen field descriptions

Commands

You may select any of the following links in the Commands field next to a telephone extension:

- Edit MS -- to go to the ***Edit Media Server screen on page 88*** for the server with that extension
- Free -- (only appears for extensions associated with users) to disassociate this extension from the user, but leave the extension available as "free" so it can be reassigned to a user in the future.
- Delete -- to go to the ***Confirm Delete Extension screen***.

Extension

(Read Only) Lists the extensions previously administered in the database.

User

(Read Only) The name of the user associated with this telephone extension, if any. Blank if "free."

Media Server

(Read Only) 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.

Host

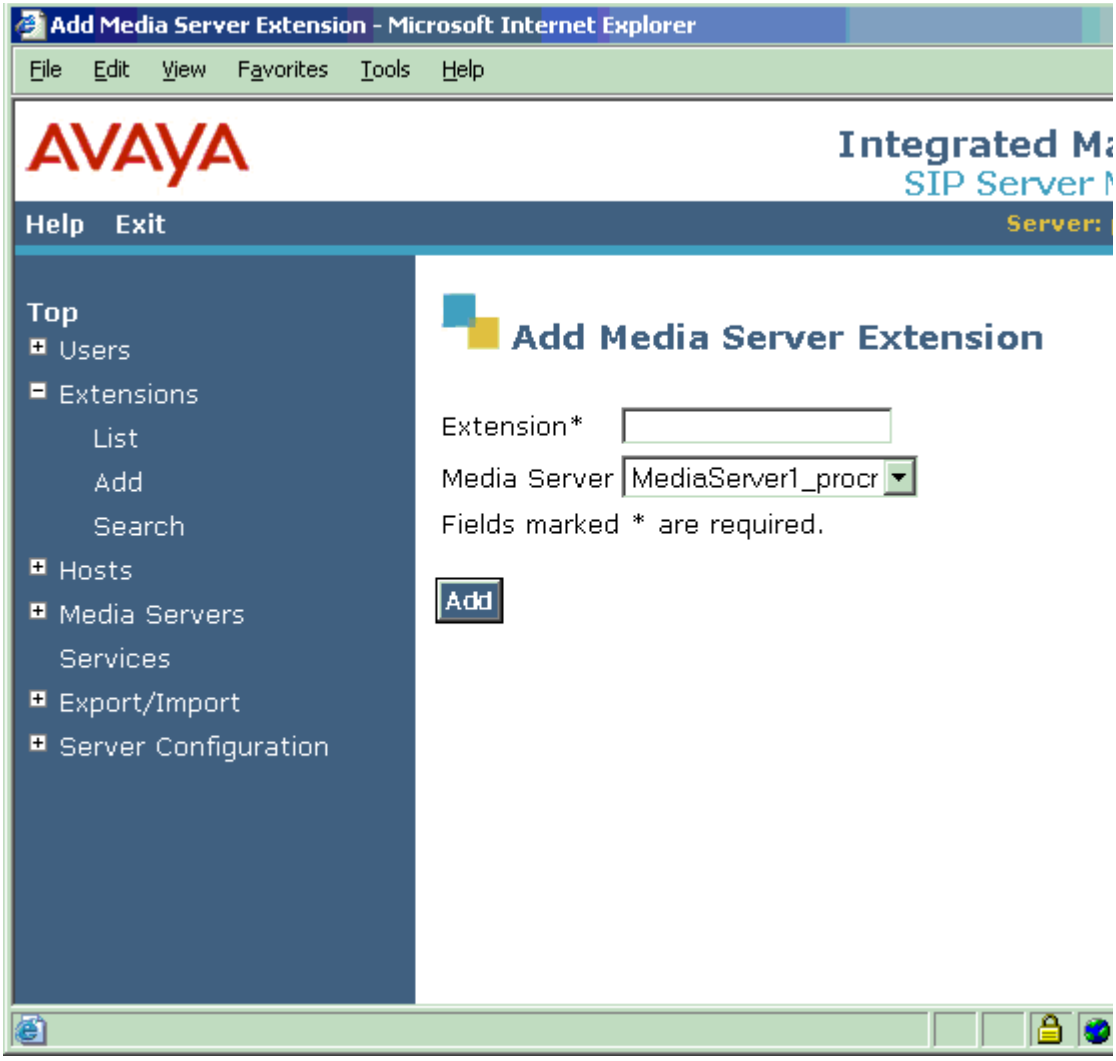
(Read Only) The network name for the server responsible for SIP traffic for this user's domain.

Select "Add Another Extension" if you want to create a new extension in the database. Select "Assign Free Extension" if you want to associate a previously administered media server extension (i.e., an extension that is now "free") with a user.

Add MS Extension screen

You can access this screen in various ways depending on context:

- By displaying it after you have checked the "Add Media Server Extension" box and submitted the ***Add User screen on page 62***
- By selecting the "Add Extension" link from the ***Manage MS Extensions screen on page 76***
- Or by selecting the "Add Another Media Server Extension" link from the ***List Media Server Extensions screen on page 78***.



Add MS Extension screen field descriptions

Extension

(Required) 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 from the drop-down list.

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 MS Extension screen

Search MS Extension screen field descriptions

Media Server

(Read Only) Select the network name of the media server you want to search from the drop-down list of media servers; by default, "any" is selected, which will search all administered media servers.

Extension

Enter the numeric telephone extension on which you want to match in the database. You can enter only a portion of the number and the results of your search will be all extensions which match the entered digits.

After you've entered your pattern criteria, select "Search" to initiate your database query.

Host screens

List Hosts screen

List Hosts screen field descriptions

Status

(Read Only) Displays a message indicating whether uncommitted updates exist since this server was last synchronized.

Commands

You may select any of the following links in the Commands field next to the name of a host:

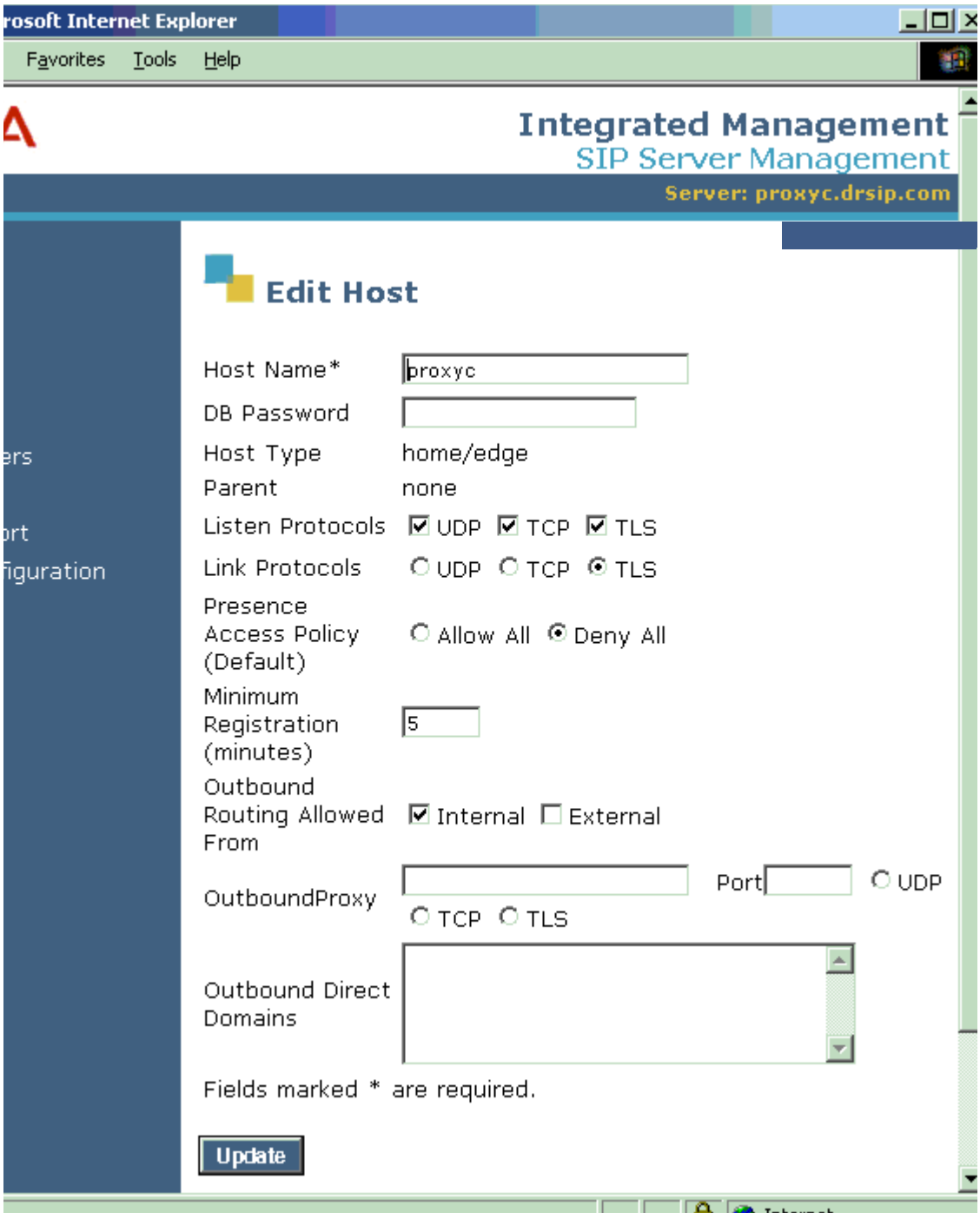
- Edit -- to go to the ***Edit Host screen on page 84*** for that server
- Map -- to go to the ***Add Address Map screen on page 89*** for that server
- Update -- (only appears if the status of this host indicates it needs to be updated)
- Go-To -- opens a separate window to display the target server's administrative web interface
- Test-Link -- opens a window with a message indicating the status of connectivity to that server
- Delete -- to delete the host. This will fail if, for example, media server(s) use this host exclusively.

Host

(Read Only) The name for this Converged Communications Server.

Select the "Update All" link to send database updates to other hosts in your system. If those databases are out of sync with the database on this host, you can select the "Force All" link to synchronize all hosts.

Edit Host screen



Edit Host screen field descriptions

Host Name

(Required) Enter the fully qualified domain name or IP address for this CCS host (server).

DB Password

(Required) Enter the password assigned to the database at installation, which should be at least 4 alphanumeric characters in length.

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 handle 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.
- {HOSTNAME} -- if the server's Host Type, above, is home, then the name of the edge proxy for all your enterprise's domains is listed as Parent.

Listen Protocols

Select any or all of the three listed protocols as protocols for which the server should listen:

- UDP (User Datagram Protocol)
- TCP (Transport Control Protocol)
- TLS (Transport Link Security)

By default, all protocols are selected to be used by the proxy to listen to/for endpoints. Note that the protocol which is selected 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

Select exactly one of the three listed protocols to be used for purposes of linking together SIP proxy hosts (home and edge servers, for instance) in your Avaya CCS system: UDP, TCP and/or TLS (the default proxy server link protocol). You must also select the Link Protocol as a Listen Protocol, above; you may want to select additional listen protocols, but you ***may not*** select any additional protocols for linking.

Minimum Registration (minutes)

Enter a whole number of minutes, 1-999, 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 5 minutes will be used.

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 handle 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. On a Home/Edge or Edge proxy server, an entry in this field typically is not required.

Outbound Port

Enter the number of the port (1-65535) on the outbound proxy server specified above that should handle 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 Transport

Select the transport protocol of the outbound proxy server that should handle SIP traffic bound for domains external to this server’s domain. TLS is recommended if the outbound proxy supports it.

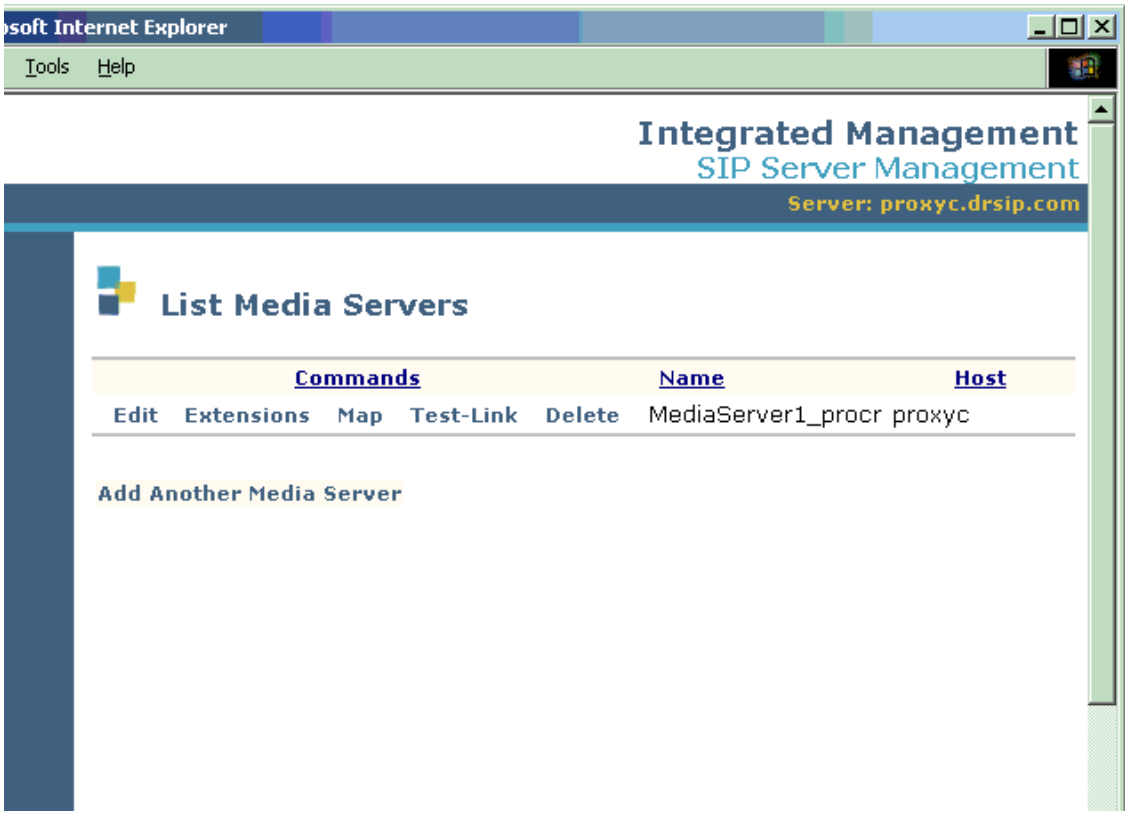
Outbound Direct Domains

List those domains for which traffic may completely bypass the Outbound Proxy server specified above. Separate entries in the list with commas, or with a white space followed by a newline, after each domain.

Select "Update" to submit to the server’s database the properties which you’ve entered or changed.

Media Server screens

List Media Servers screen



List Media Servers screen field descriptions

Commands

You may select any of the following links in the Commands field next to a media server's name:

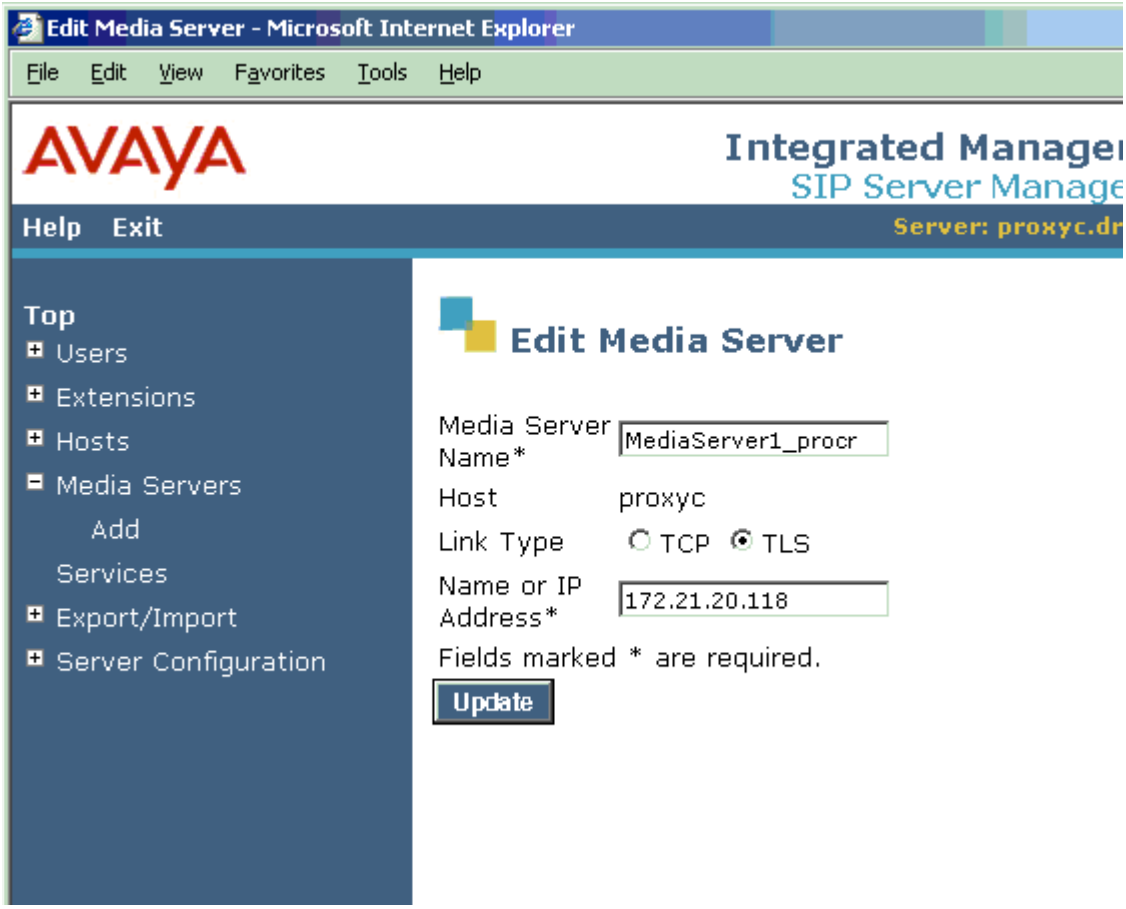
- Edit -- to go to the ***Edit Media Server screen on page 88*** for that server
- Extensions -- to go to the ***List Media Server Extensions screen on page 78*** for that media server
- Map -- to go to the ***Add Address Map screen on page 89*** for that media server
- Test-Link -- opens a window with a message indicating the status of connectivity to that server.
- Delete -- to go to the ***Confirm Delete Media Server screen*** to verify that you want to delete it.

Host

(Read Only) The alphanumeric name for this Converged Communications Server.

To administer a new media server in the proxy host's database, select "Add Another Media Server.".

Edit Media Server screen



Edit Media Server screen field descriptions

Media Server Name

(Required) Enter a friendly name in alphanumeric characters referencing 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.

Host

(Read Only) Displays the proxy host 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.

Name or IP Address

(Required) The IP address for the media server's CLAN (or processor CLAN), specified as a 32-bit address comprising 4 8-bit octets (i.e., each 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.

Select "Update" to submit the properties you've reviewed/changed for this media server.

Add Address Map screen

Add Address Map screen field descriptions

NOTE:
An address map should identify messages allowed between CCS and the media server over the SIP trunk administered in Avaya Communication Manager. Map patterns should be devised 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) Displays the name of the media server to which this address map applies.

Name

(Required) Enter an alphanumeric name to identify the map you are adding. 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 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).

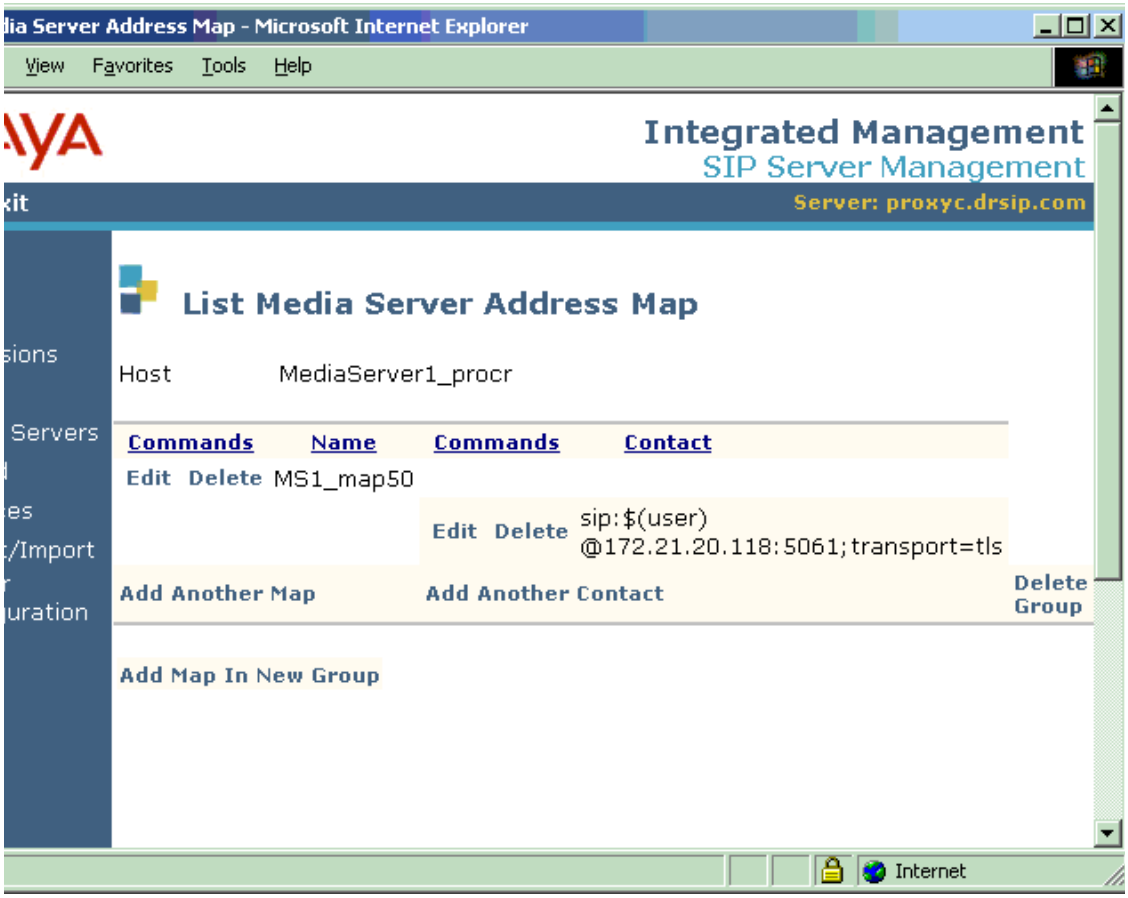
For more information, refer to "*SIP Support in Avaya Communication Manager*", Doc ID 555-245-206.

Replace URI

In case the contact information in this map is that of an endpoint (e.g., a SIP phone or a user on a media server running Communication Manager), then this box should be checked for "yes." 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 proxy to forward requests to another entity (i.e., another SIP proxy server) for that other entity to resolve the contact and route the request, then uncheck the "Replace URI" box.

After completing the fields, select "Add" to submit the address map entry to the database on this host.

List Address Map screen



List Address Map screen field descriptions

Address Maps are listed in groups and associated with Media Servers and the extensions on them.

Host

(Read Only) Displays the name of the media server to which the agroup(s) of address map(s) apply.

Commands

You may select any of the following links in the Commands field next to a map's Name or an associated Contact:

- Edit -- to go to the ***Edit Map Entry screen on page 93*** for that map or the ***Edit Contact screen on page 95*** for that Contact in the database.
- Delete -- to go to the ***Confirm Delete Map*** screen for that map or the ***Confirm Delete Contact*** screen for that Contact in the database.

Name

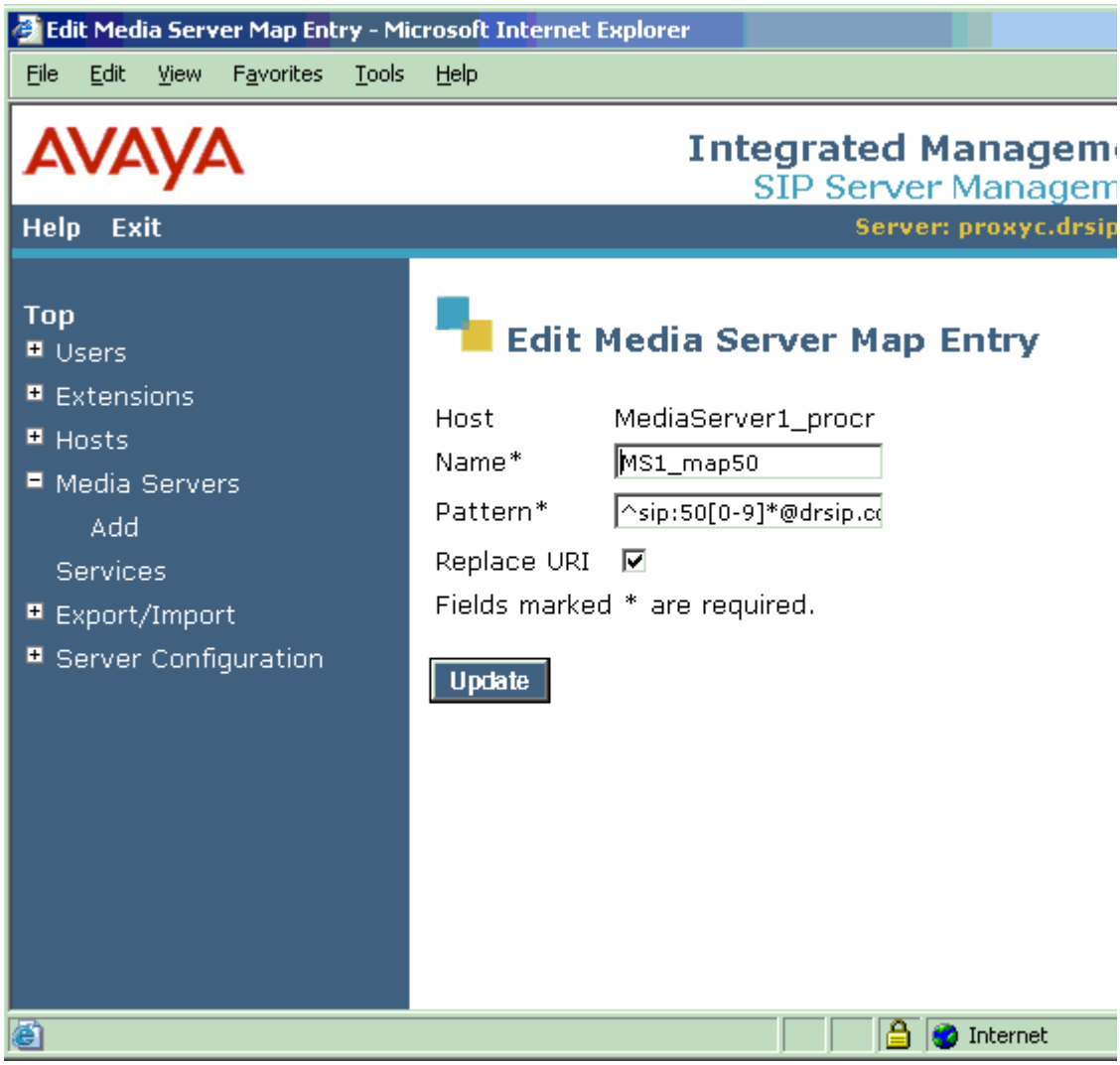
(Read Only) Displays the name specified for this address map in the database.

Contact

Contact entries may be fixed (constant data you enter after selected "Edit") or dynamically constructed by the system. In the example shown, the CCS 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.

Select the "Add Another Map" link to add another address map in this same group. Select "Add Another Contact" to create another contact for the same address map. Select the "Delete Group" link to remove this group of address map(s) from the database. Or select the "Add Map in New Group" link to create a new map in a new group.

Edit Map Entry screen



NOTE:
An address map should identify messages allowed between CCS and the media server over the SIP trunk administered in Avaya Communication Manager. Map patterns should be devised 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 Map Entry screen field descriptions

Host

(Read Only) Displays the name of the media server to which this address map applies.

Name

(Required) Enter an alphanumeric name to identify the map you are adding. 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 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).

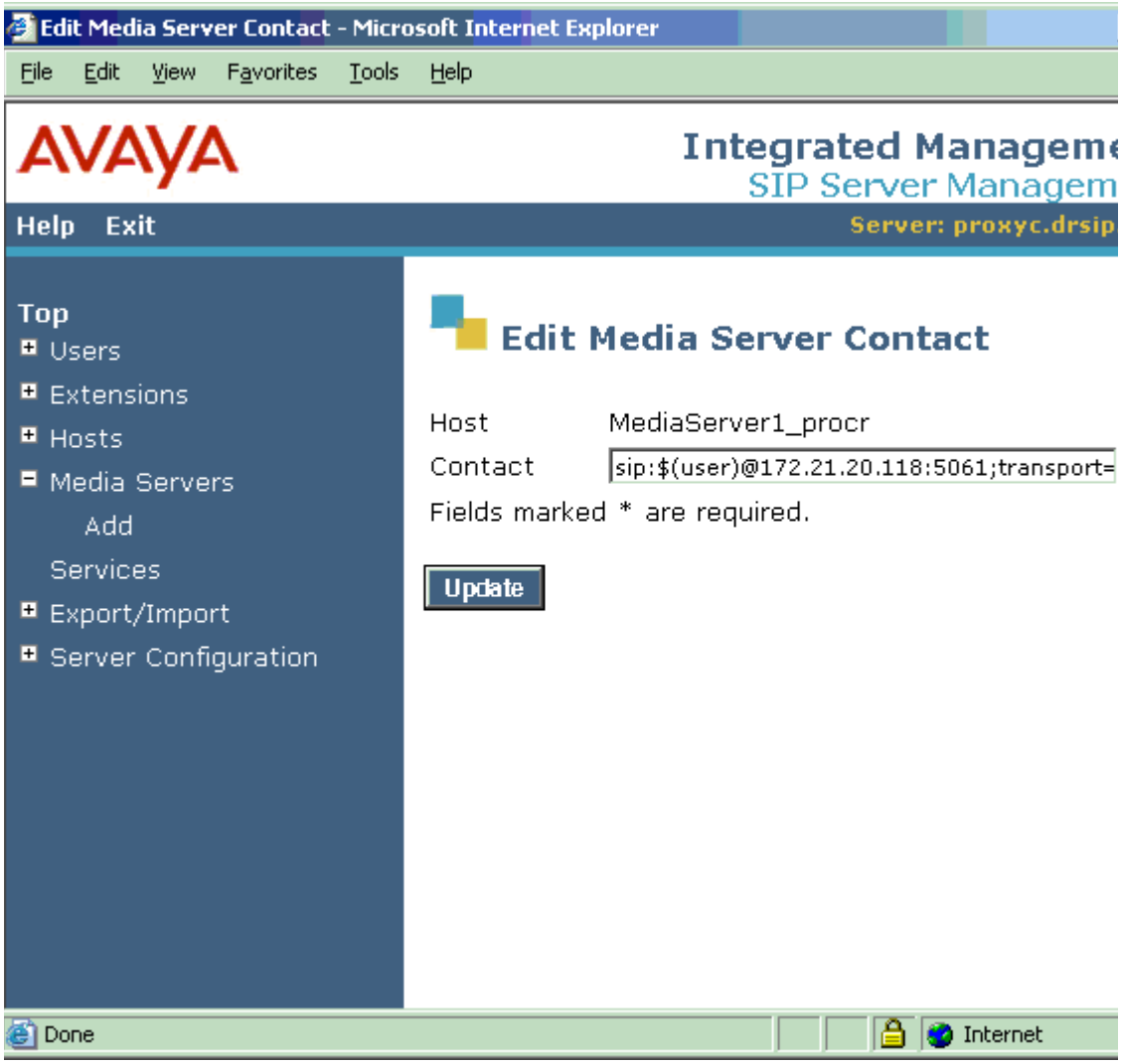
For more information, refer to "*SIP Support in Avaya Communication Manager*", Doc ID 555-245-206.

Replace URI

In case the contact information in this map is that of an endpoint (e.g., a SIP phone or a user on a media server running Communication Manager), then this box should be checked for "yes." 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 CCS proxy to forward requests to another entity (i.e., another SIP proxy server) for that entity to resolve the contact and route the request, then uncheck the "Replace URI" box.

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.

Edit Contact screen



Edit Contact screen field descriptions

Host

(Read Only) Displays the name of the media server to which this contact applies.

Contact

When a match for an address map is found, the associated Contact may be a fixed destination, or it may be constructed dynamically to 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 URI (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.

After reviewing and/or changing it, select the Update button to submit the entry to the host database.

Services screen

Services Administration screen

Services Admin 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 a normal state for a properly functioning server
- DOWN (or Stopped) -- if this service is not running on this host; this message may inidcate a problem with the server, its installation or configuration.

Commands

You may select any of the following links in the Commands field next to a telephone extension:

- Start -- to start this service on this host, if it is not running
- Stop -- to stop this service on this host, if it is running
- Restart -- to stop and then start this service on this host, if it is running. You may want to select this link if a service appears to be hung, and is not responding to requests.

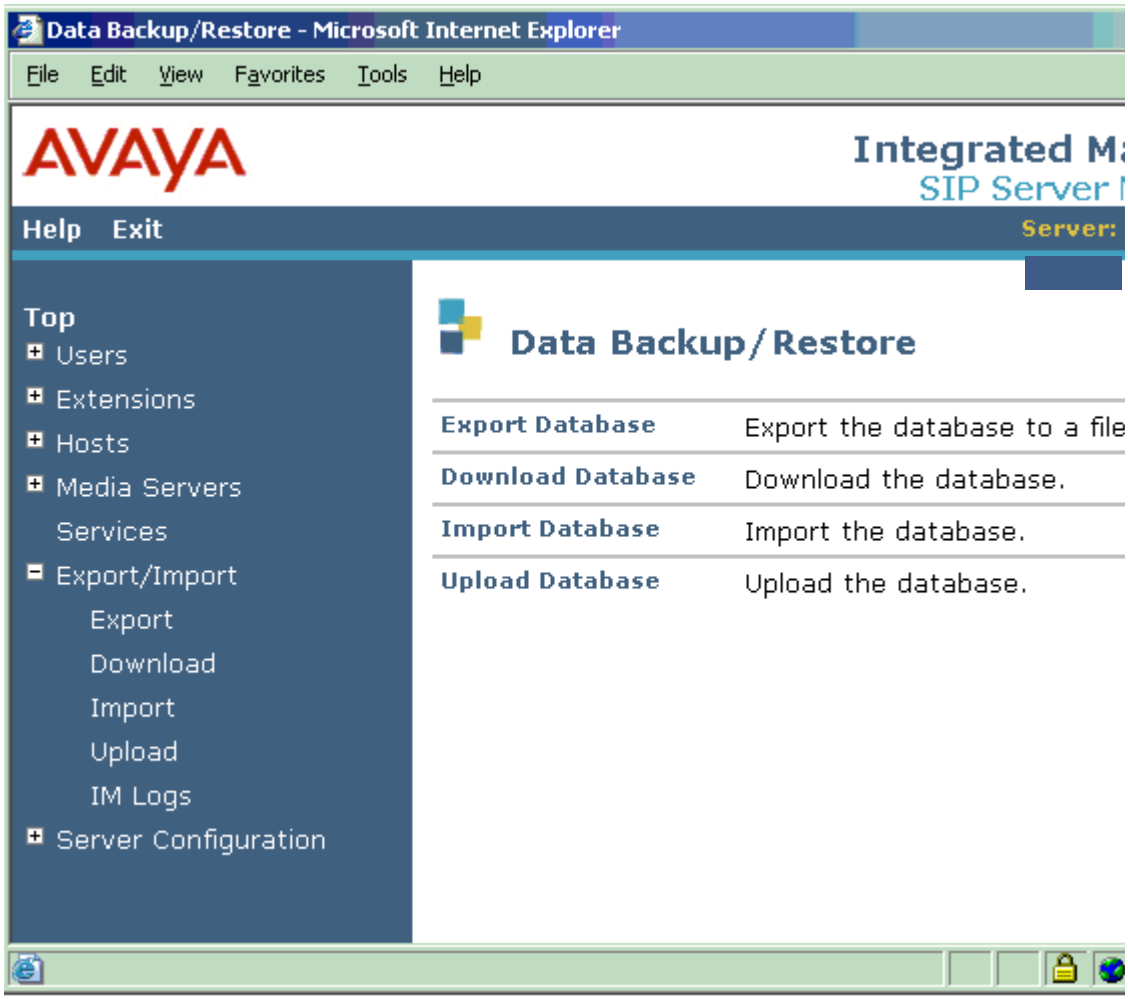
Server

(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

Export/Import Screens

Export/Import screen



Export/Import screen field descriptions

Export Database

Select this link to export the host's database to a file in the /tmp/ directory on the Linux system (see the following illustration).

Download Database

Select this link to copy the host server's database to a file which you can save on your local computer.

Import Database

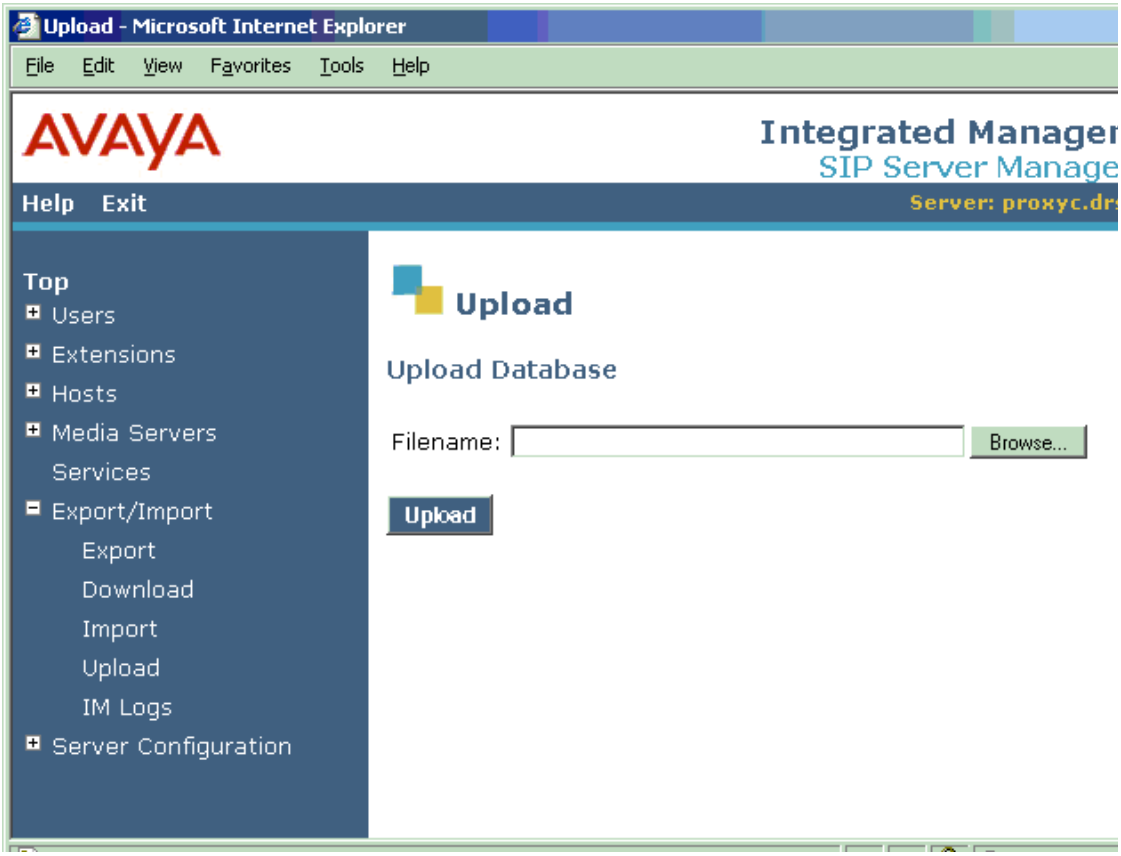
Select this link to import a host server database from a file in the /tmp/ directory on the Linux system

Upload Database

Select this link to upload a copy of the host's database from a file saved on your local computer. You can select "Browse" to aid in locating and entering the full pathname to the filename.

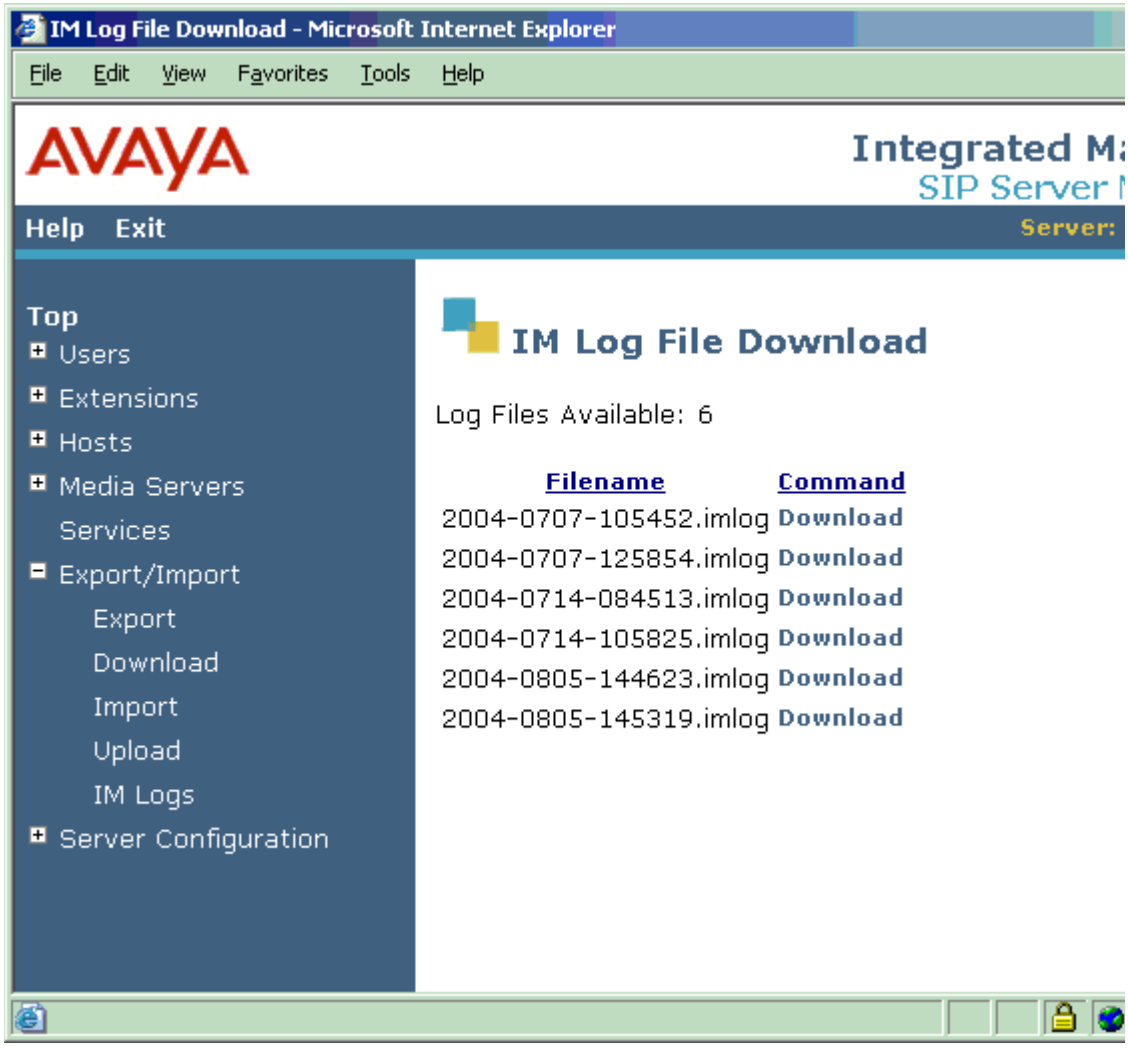
NOTE:
Both the Import and Upload functions completely delete and replace any existing database. The merging of multiple server databases is not supported.

Upload Database screen



After entering (or browsing for) the pathname to the database file, select the Upload button.

IM Logs screen



IM Logs screen field descriptions

Filename

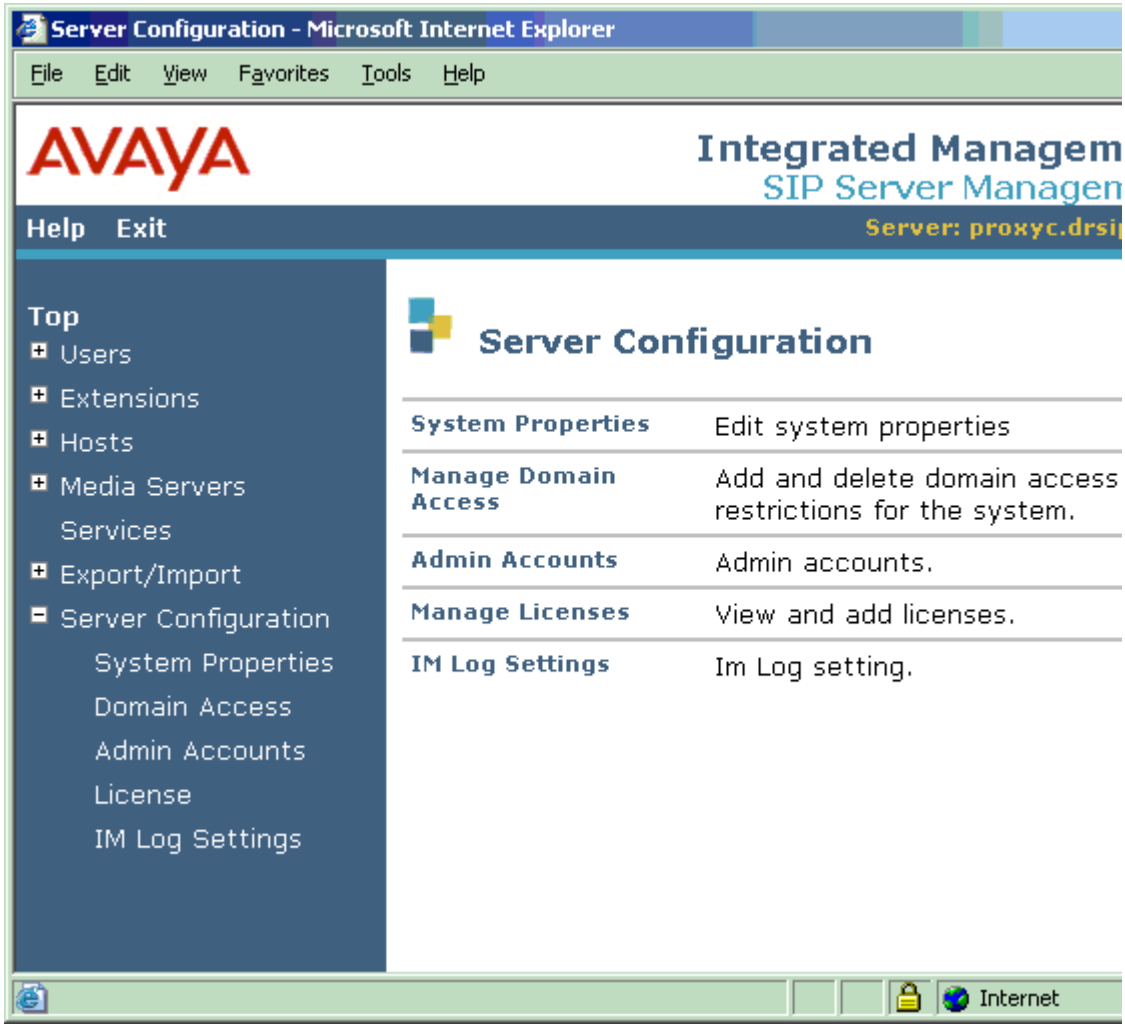
Each log file is named with its creation date (YYYY-MMDD) and timestamp (HHMMSS). A new file is not automatically created at any specific time or interval, but when the existing file reaches the maximum size for an IM log file, administered in kilobytes (KB) on the IM Log Settings screen on page 114.

Command

Select the link for the Download command to the right of the log filename you wish to download.

Server Configuration screens

Server Configuration screen



Server Configuration screen field descriptions

System Properties

Select this link to go to the ***Edit System Properties screen*** on page 49 and, for example, setup the server's domain.

Manage Domain Access

Select this link to go to the ***List Domain Access screen on page 105*** and view or add another entry in the access list.

Admin Accounts

Select this link to go to the ***List Administrators screen on page 109*** and edit, delete or add a new administrative login account.

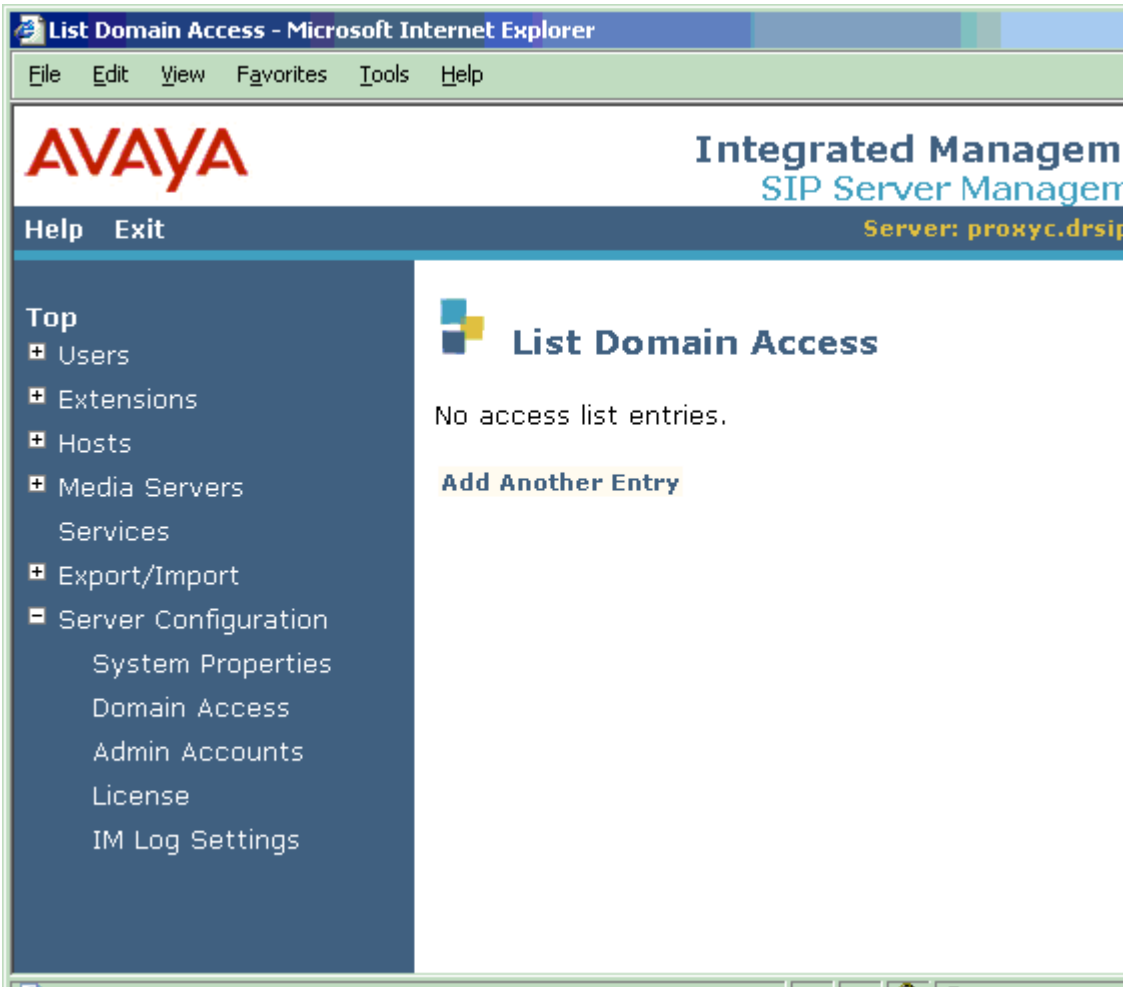
Manage Licenses

Select this link to go to the ***Manage Licenses screen on page 112*** 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 114 and view or set the IM Log or its properties.

List Domain Access screen



List Domain Access screen field descriptions

Commands

You may select any of the following links in the Commands field next to a domain access entry:

- Edit -- to go to the ***Edit Domain Access*** screen for that entry.
- Delete -- to go delete this domain access entry from the server.

Direction

(Read Only) Shows In and/or Out for the access direction this entry defines.

Domain

(Read Only) Shows the network name of the domain, traffic for which is defined by this entry.

Action

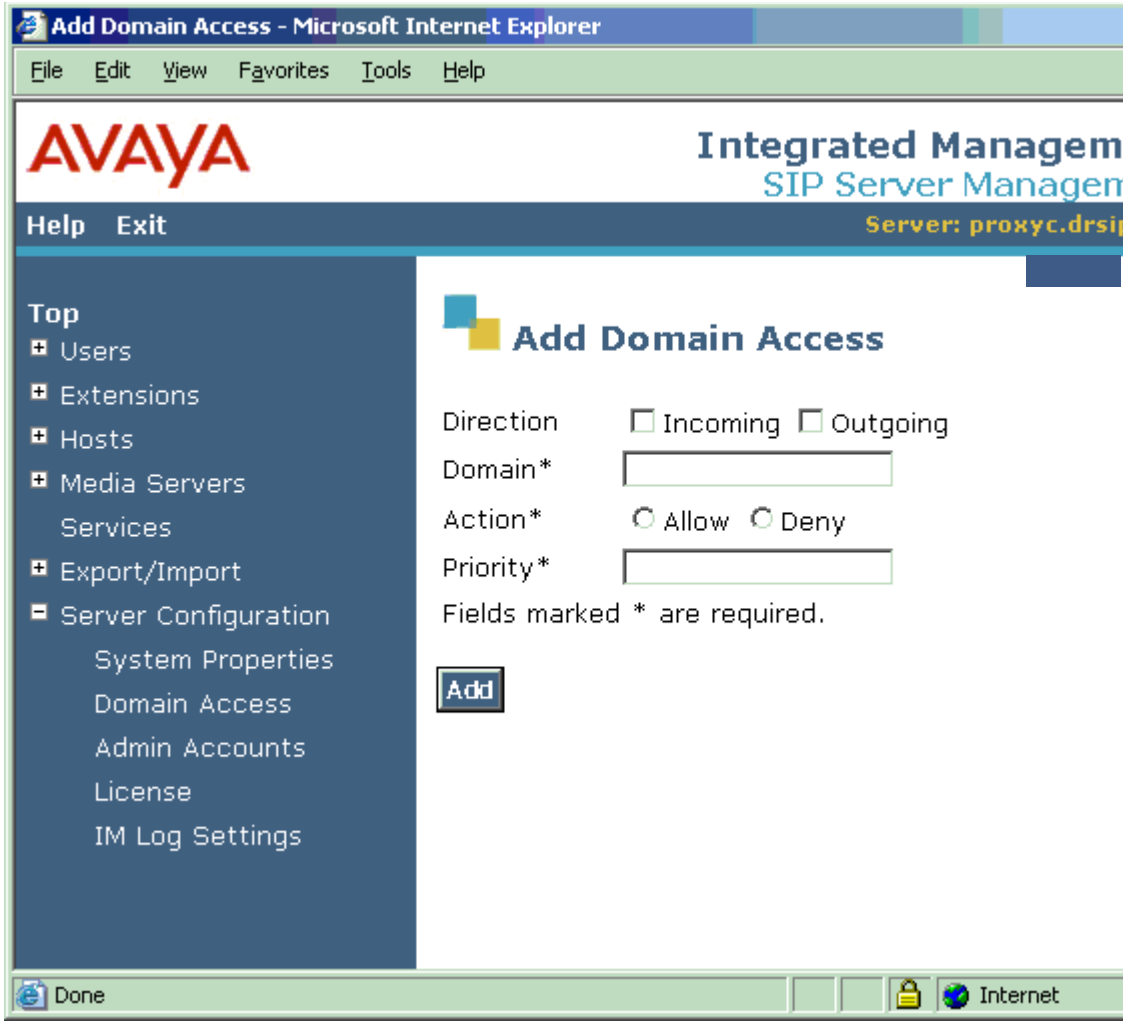
(Read Only) Show either Allow or Deny according whether SIP traffic can be routed to and/or from the domain specified above.

Priority

(Read Only) Shows a whole number representing the relative priority this entry has.

Select the "Add Another Entry" link to go to the ***Add Domain Access*** screen and create a host entry.

Add Domain Access screen



Add Domain Access screen field descriptions

Direction

Select Incoming and/or Outgoing 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 mimimum of one direction.

Domain

(Required) Enter the alphanumeric name of the domain for which traffic is to be defined by this entry.

Action

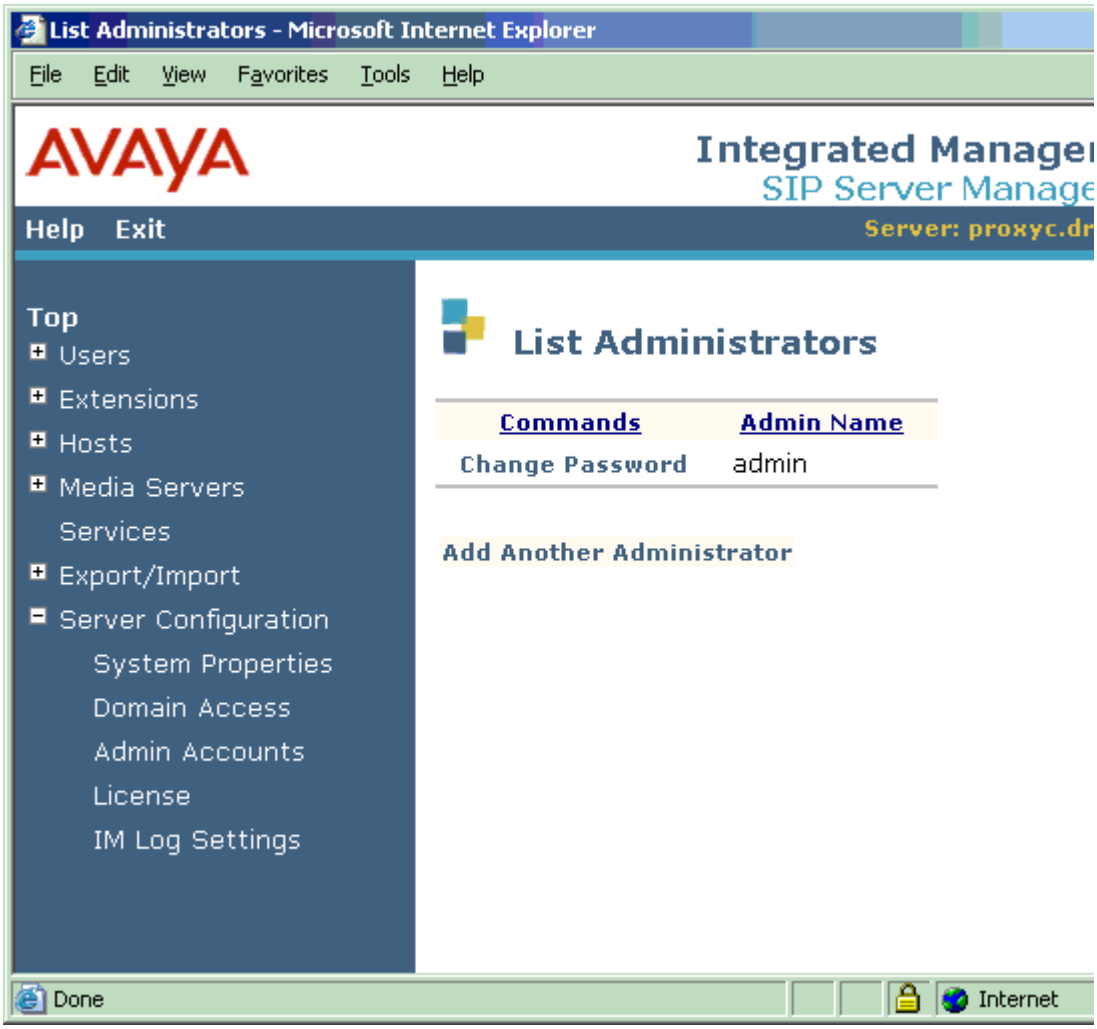
(Required) Select either Allow or Deny to specify whether SIP traffic can be routed to and/or from the domain specified above.

Priority

(Required) Enter a whole number representing the priority this entry has relative to other database entries.

Select the "Add" button to submit a domain access entry with the properties you've entered on this host.

List Administrators screen



List Administrators screen field descriptions

Admin Name

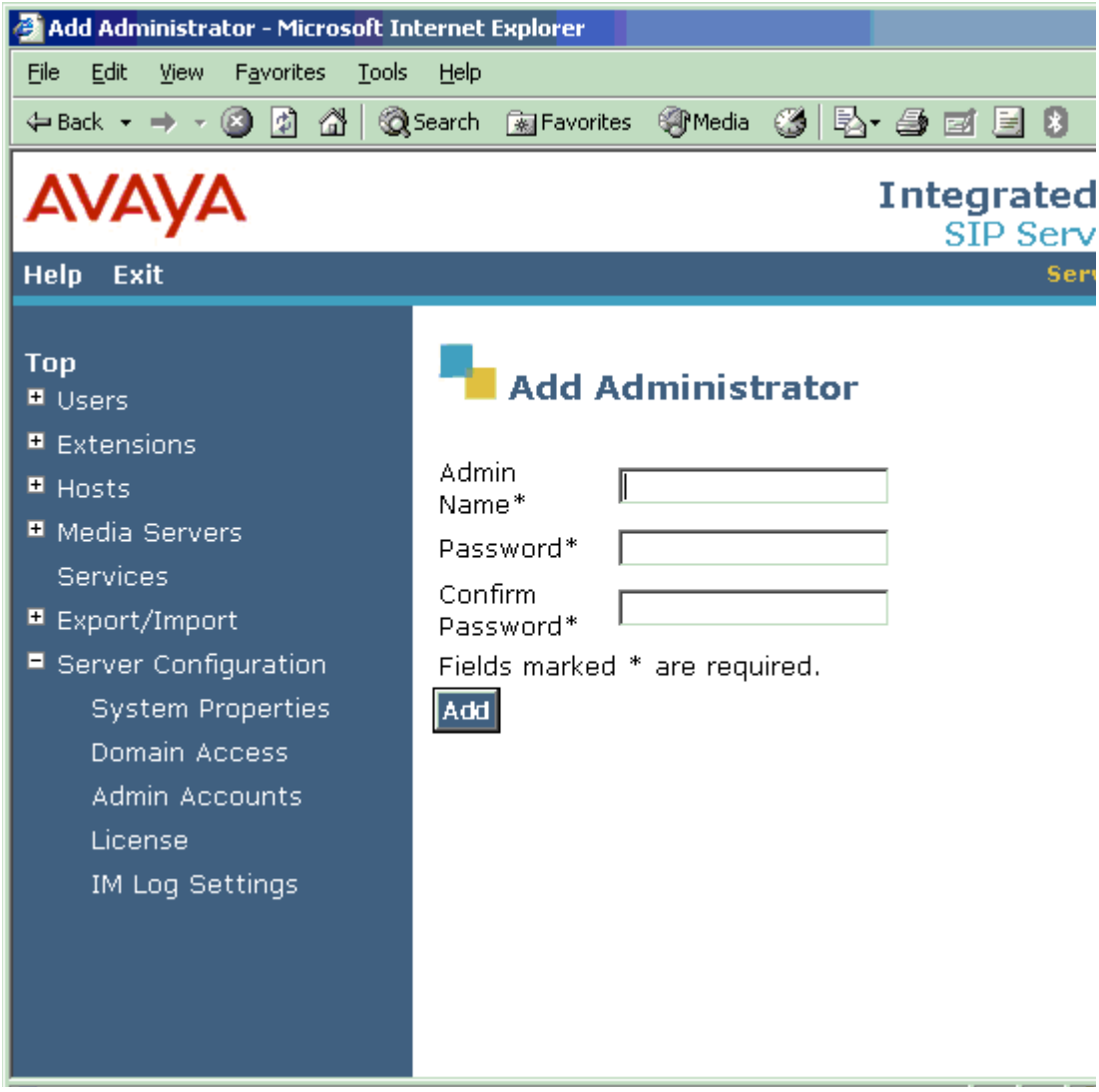
(Read Only) Lists the login names of previously administered accounts with administrative rights.

Commands

You may select the Change Password link next to an Admin Name to go to the ***List Administrators screen on page 109*** for that administrator. If more than one account is listed with administrative rights, then you may select the Delete link next to an Admin Name to delete the associated account.

Or you may select "Add Another Administrator" to go to the ***Add Administrator screen on page 110***.

Add Administrator screen



Add Administrator screen field descriptions

Admin Name

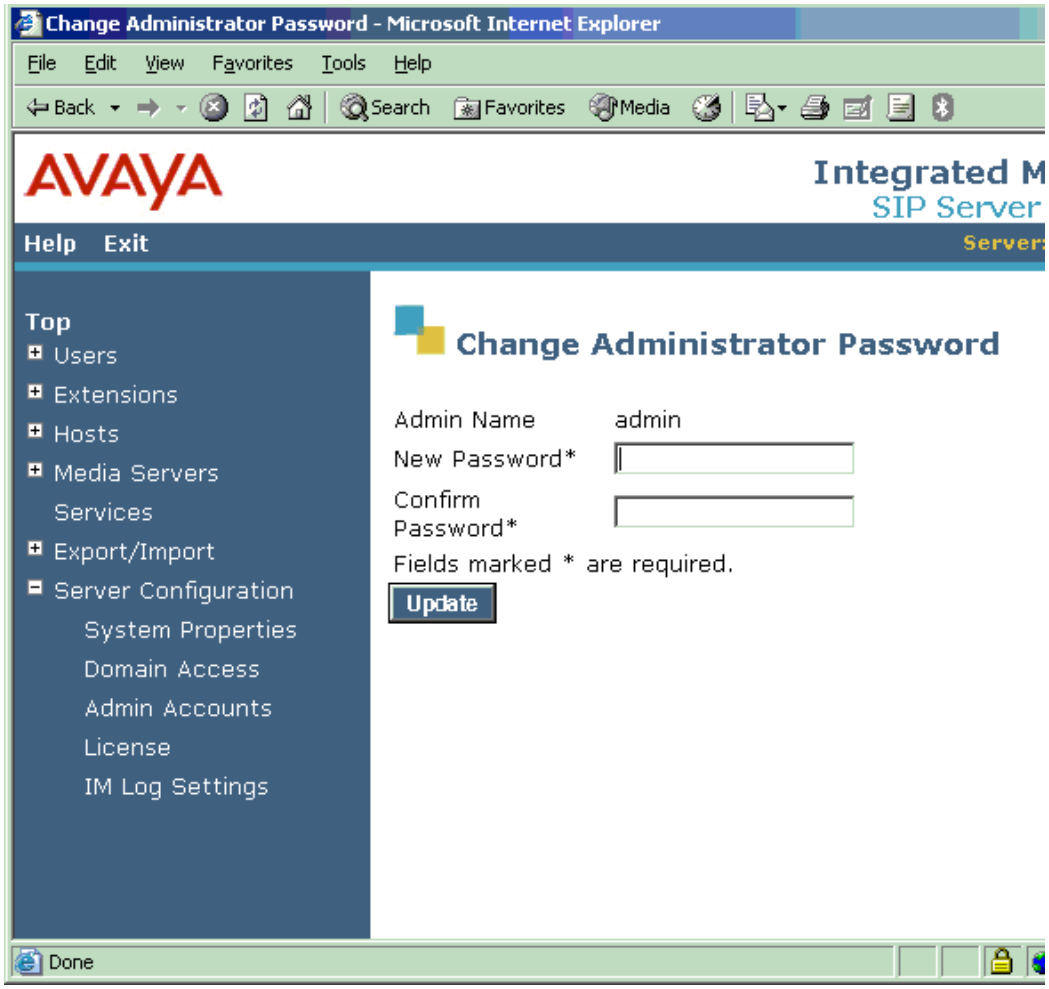
(Required) Enter a login name for the new administrator, of at least 3 alphanumeric characters in length.

Password, Confirm Password

(Required) Enter a password of at least 6 characters, at least 1 of which is alphabetic and at least 1 of which is numeric; your entries in both of these fields must match exactly.

After completing these fields, select "Add" to add an administrative account.

Change Administrator Password screen



Change Admin Password screen field descriptions

Admin Name

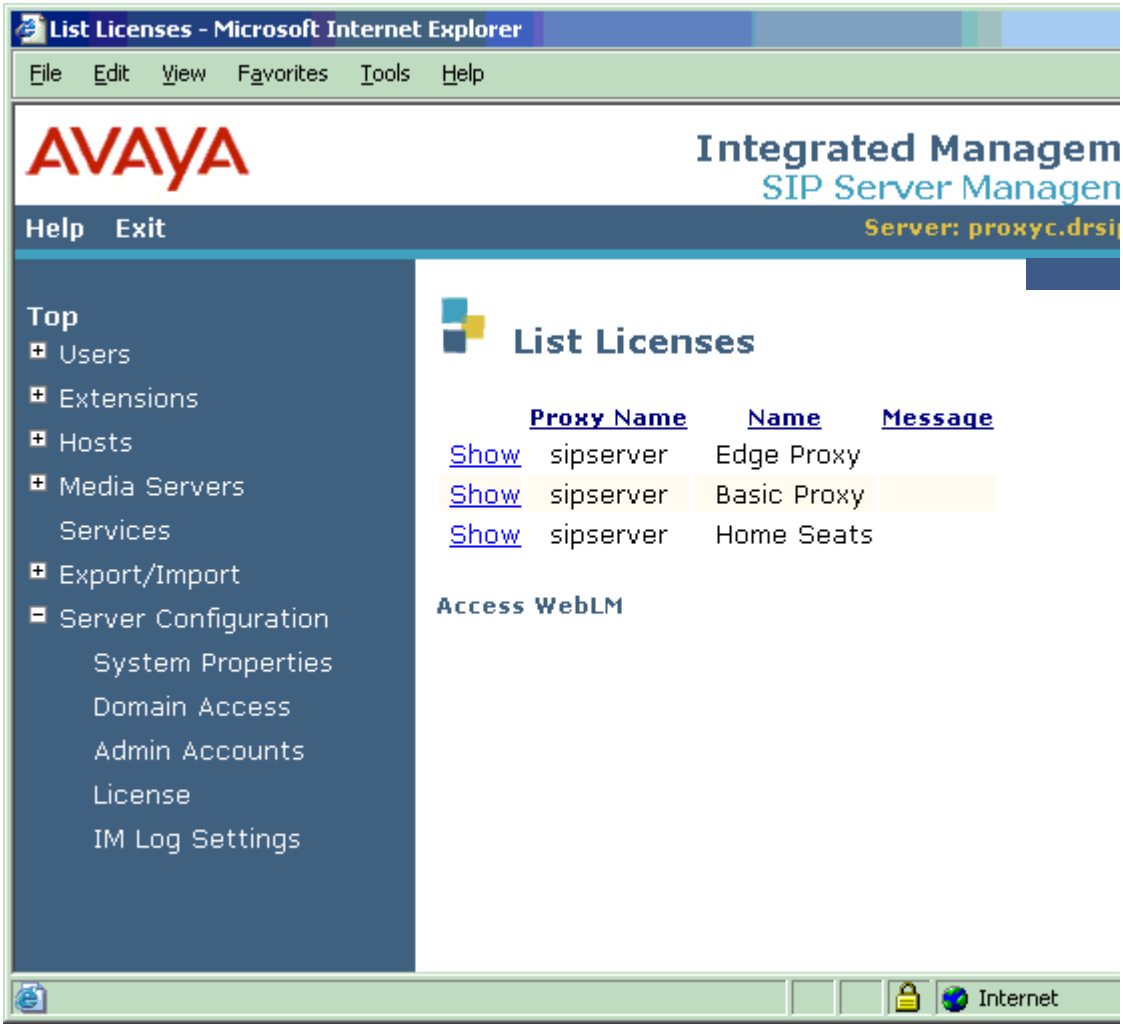
(Read Only) Displays the logon ID of the administrator for whom you are changing the password.

New Password, Confirm Password

(Required) Enter the new password of at least 6 characters, at least 1 of which is alphabetic and at least 1 of which is numeric; your entries in both of these fields must match exactly. Asterisks will be displayed.

After completing these fields, select "Update" to submit the change to the database on this host.

Manage Licenses screen



Manage Licenses screen field descriptions

Show

Select this link to display status information about a specific license.

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 which are licensed for this Avaya Converged Communications Server. Duplex server configurations are licensed as one Active host. The licensed proxies include:

- Basic Proxy -- each CCS 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, per CCS system.
- Home Seats. -- Each administered user in the CCS 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, typically in 10 days.

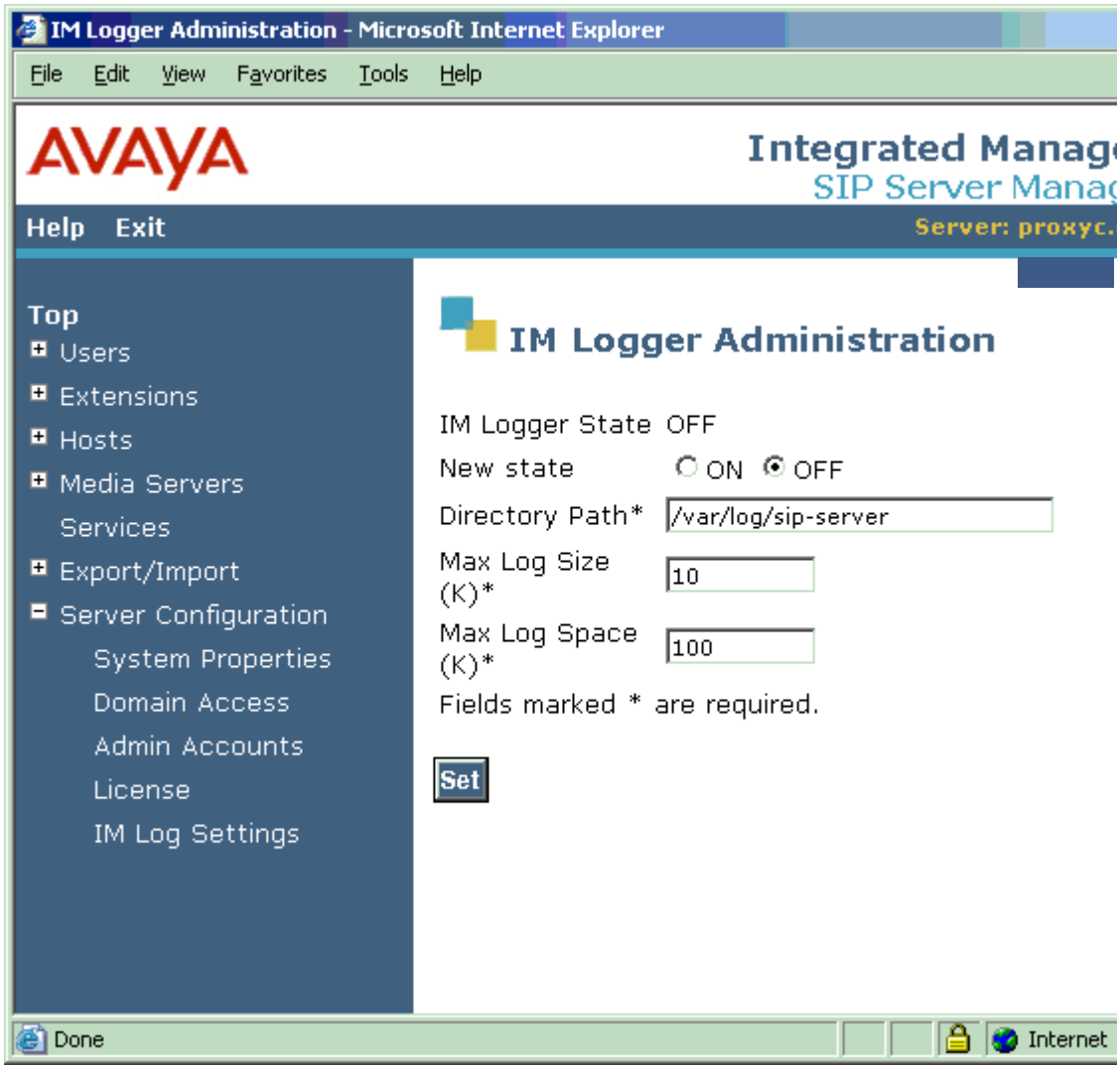
If you need to activate an existing license on this server, select the "Access WebLM" link.

IM Log Settings screen

Tip:

The following tips will help you administer the IM Logger application:

- A new IM Log file is created whenever IM Logger starts.
- This file is used to log instant messages until it reaches the maximum size for an IM log file, administered in kilobytes (K bytes).
- A message is recorded in the log file whenever logging is enabled and disabled from this adminstration 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.



IM Log Settings screen field descriptions

IM Logger State

(Read Only) This field shows the current state of the IM Logger as OFF or ON.

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 pathname to the directory to which 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 10KB, 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 than the number entered in the Max Log Space field, 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 100KB, or approximately 10 of the maximum-sized IM log files specified by default. You can change this ratio, so long as the number entered here is larger than the number entered in the Max Log Size field, above.

After you have entered the properties for IM Logger, select "Set" to submit them to this server.

4 Maintenance Web Interface

List of Screens

The following screens are used to maintain a Converged Communications Server. (Note that many of these screens only are applicable to servers running the Master interface, typically those that are set up as an Edge or as a combined Home/Edge proxy; the administrative capabilities of Home servers typically are limited to a subset of Services and Export/Import Tasks.)

Top

At the top-most level of the Master web interface are the following:

- ***Logon screen on page 119***
- ***Choose Interface screen on page 120***

  Select the link to "Launch Maintenance Web Interface" and the following choices appear.

Alarms

The names of the screens (and of the links to them) pertaining to Alarms are as follows:

- ***Current Alarms screen on page 121***
- ***SNMP Traps screen on page 124***

Diagnostics

The names of the screens (and of the links to them) pertaining to Diagnostics are as follows:

- ***System Logs screen on page 126***
- ***Temperature/Voltage screen on page 129***
- ***Ping screen on page 132***
- ***Traceroute screen on page 134***
- ***Netstat screen on page 138***
- ***Modem Test screen on page 142***

Server

The names of the screens (and of the links to them) pertaining to the Server are as follows:

- ***Status Summary screen*** on page 144
- ***Process Status screen on page 146***
- ***Shutdown Server screen on page 149***

- *Server Date/Time screen on page 151*
- *Software Version screen on page 153*

Server Configuration

The name of the screen (and of the link to it) pertaining to Server Configuration is as follows:

- *Eject CD-ROM screen on page 154*

Server Upgrades

The names of the screens (and of the links to them) pertaining to Server Upgrades are as follows:

- *Install New Software screen on page 155*
- *Make Upgrade Permanent screen* on page 162
- *Boot Partition screen* on page 164

Data Backup/Restore

The names of the screens (and the links to them) pertaining to Data Backup and Restore are as follows:

- *Backup Now screen* on page 167
- *Backup History screen on page 170*
- *Schedule Backup screen on page 171*
- *Backup Logs screen on page 174*
- *View/Restore Data screen* on page 176
- *Restore History screen on page 178*
- *Format PC Card screen* on page 179

Security

The names of the screens (and of the links to them) pertaining to Security are as follows:

- *Modem screen on page 180*
- *FTP screen on page 182*
- *Firewall screen on page 185*
- *WebLM Software screen* on page 189
- *WebLM License Admin screen* on page 190
- *Tripwire screen on page 192*
- *Tripwire Commands screen on page 194*
- *Install Root Certificate screen on page 195*
- *SSH Keys screen on page 196*

Miscellaneous

The name of the Miscellaneous screen (and of the link to it) is as follows

- ***Download Files screen on page 198***

Top-Level Screens

Logon screen

Logon screen field descriptions

Logon ID

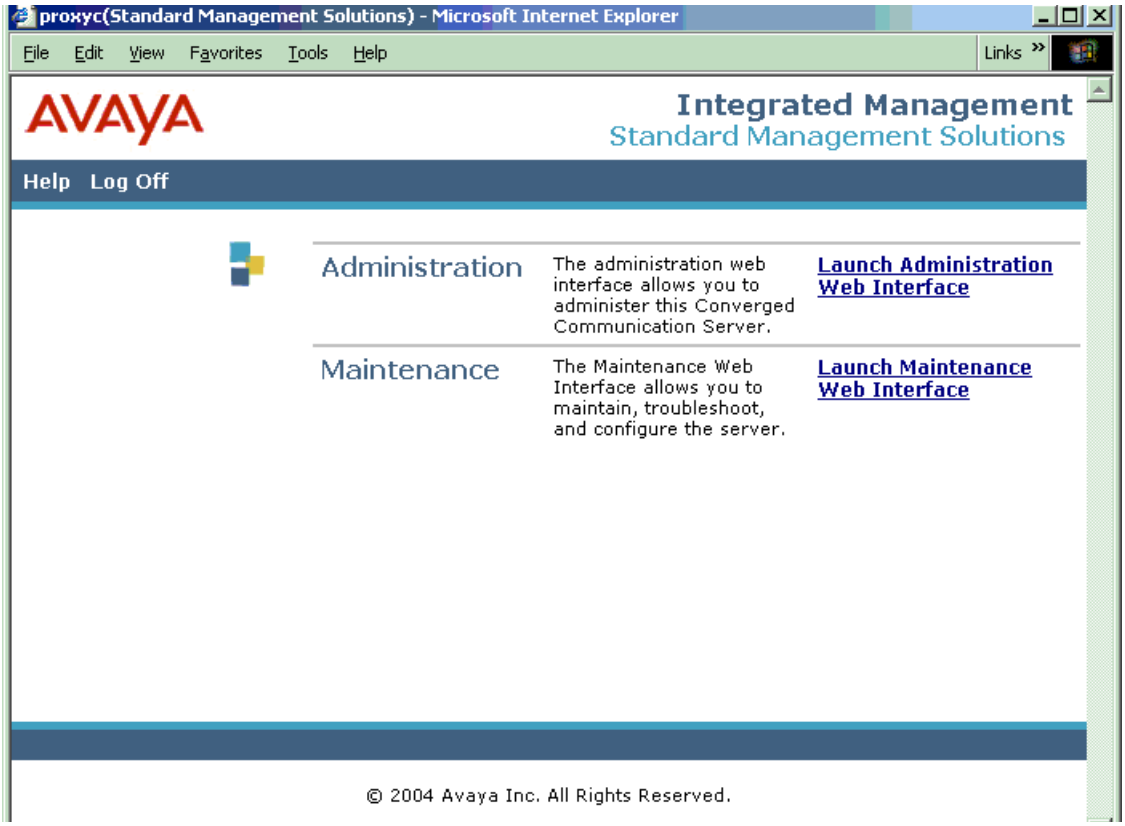
(Required) Enter the user name with which to log on to your administrative account. After you enter this name andpress the Return key or select Logon, the screen will refresh with the following Password field.

Password

(Required) Enter your adminstrative account's password, at least 7 characters in length, at least 1 of which is alphabetic and at least 1 numeric.

After completing both fields, select "Logon" or press the Enter or Return key on your keyboard.

Choose Interface screen



Choose Interface screen field descriptions

Use the Choose Interface screen after logon to select from either the Administration Web Interface or the Maintenance Web Interface, depending on what functions you need to perform on the server.

Administration

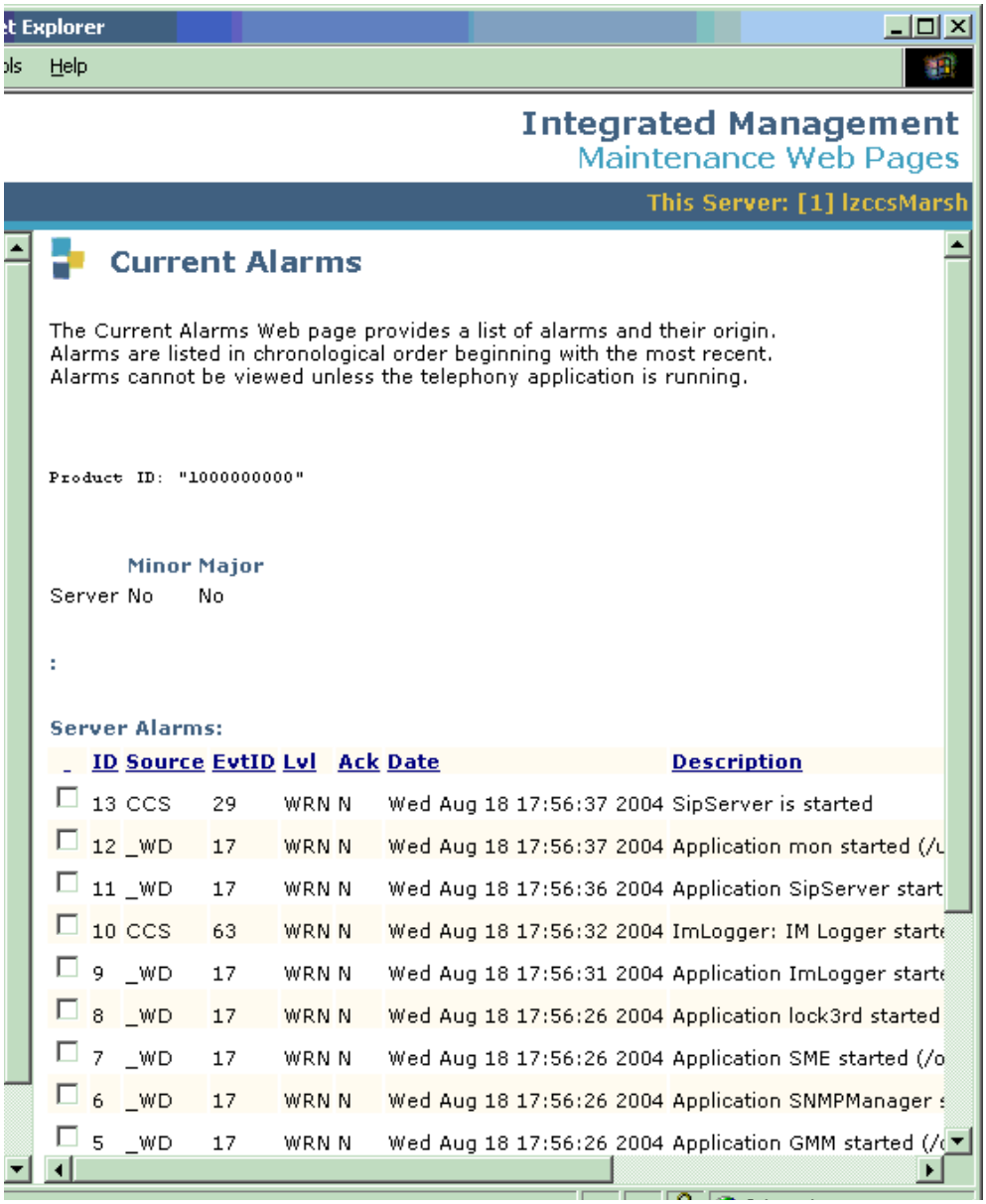
The administration interface is used for initial server setup, user contact database changes and media server related activities. Select the link to the right to "Launch Administration Web Interface."

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."

Alarms screens

Current Alarms screen



Current Alarms screen field descriptions

Use the Current Alarms page to view a list of outstanding alarms against Converged Communications Server (CCS) software. This page shows either a summary of alarms, if present, or a message stating that no alarms are present.

Product ID

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 identificaion number assigned to the alarm.

Source

This is the abbreviated name of the software module that generated the alarm, as follows:

- **ENV** for environment
- **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

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" 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.

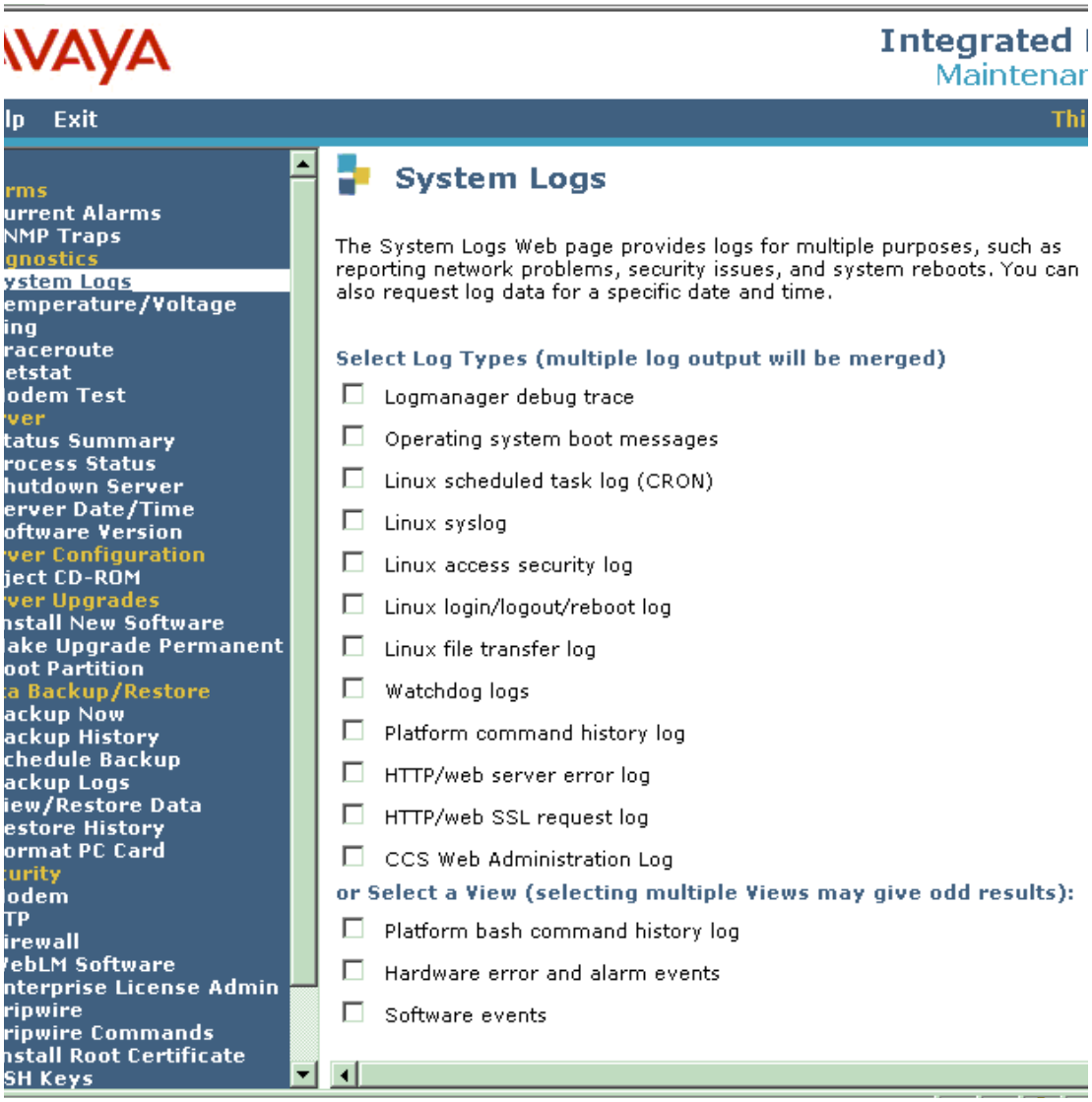
The SNMP Trap page may display the following error:

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

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.



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 Converged Communications Server 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, heartbeating, 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.
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.

Log Type	Description
ccsadmin	**Converged Communications Server Web Administration log**. The last 16 administrative functions performed on the CCS 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 logview* 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 Converged Communication Server's hardware error and alarm logs.
swerr	**Software events**. The events that go into the Converged Communications Server's software error log.

Select Event Range

1. Select one of the following 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

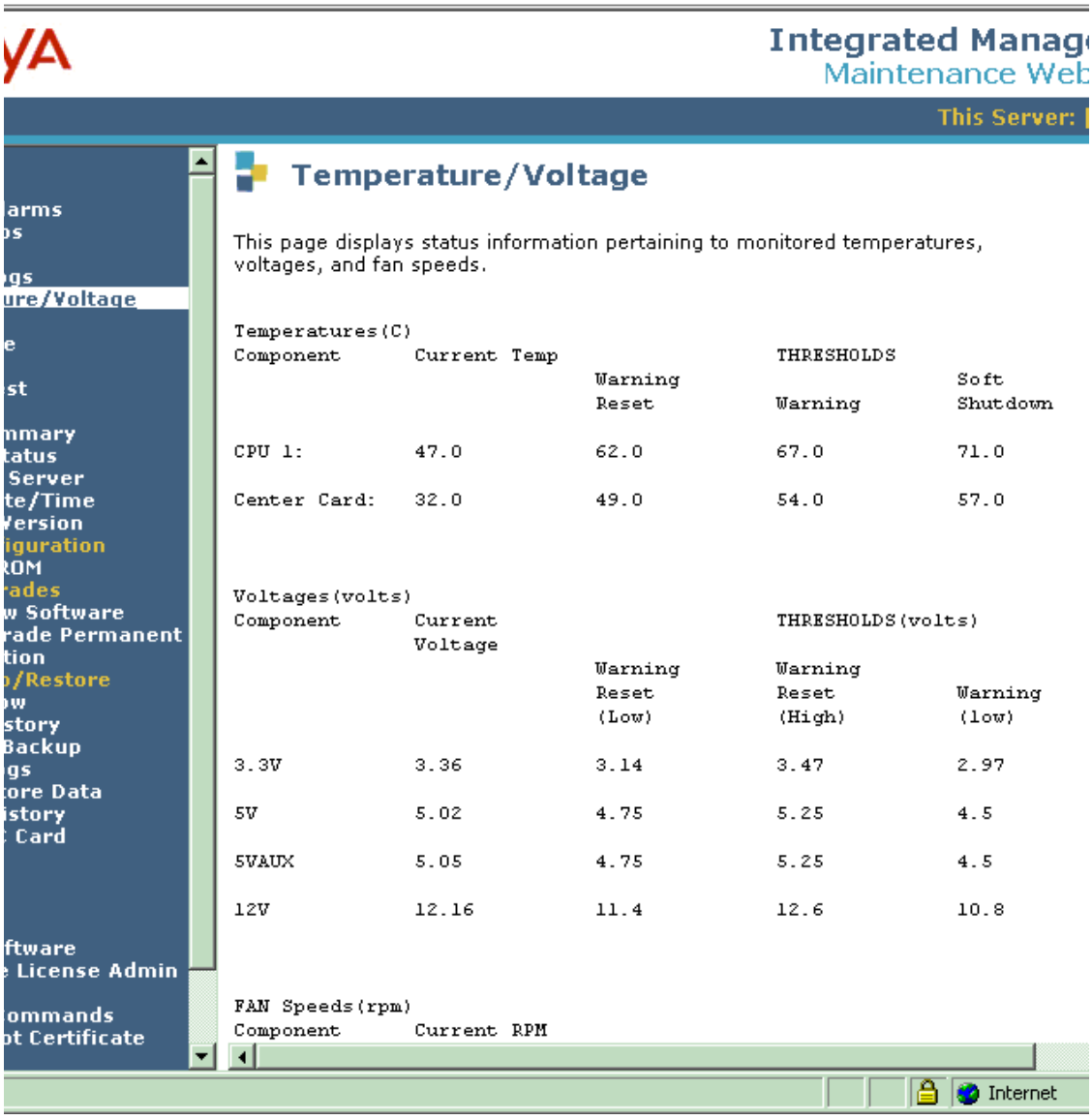
(Optional) To further limit your search, enter a keyword in the Match pattern field (such as a name or message type). The log will display only those entries that contain this keyword. You must check the box to the left of this field to search for entries with this keyword.

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



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.

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 caused an alarm, you can 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.

Ping screen


Integrated Manag
Maintenance Web
This Server:
Ping
The Ping Web page provides useful network debugging. Use the host name or the IP address and execute a Ping command to determine whether a specific network address is valid, and obtain information about processing data packets and diagnostics to troubleshoot problems.
Endpoints to Ping
Host Name Or IP address
UPS endpoints.
Options
Do not look up symbolic names for host addresses.
Bypass normal routing tables and send directly to a host.
Execute Ping
Help
Internet

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 Uninterruptable 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.

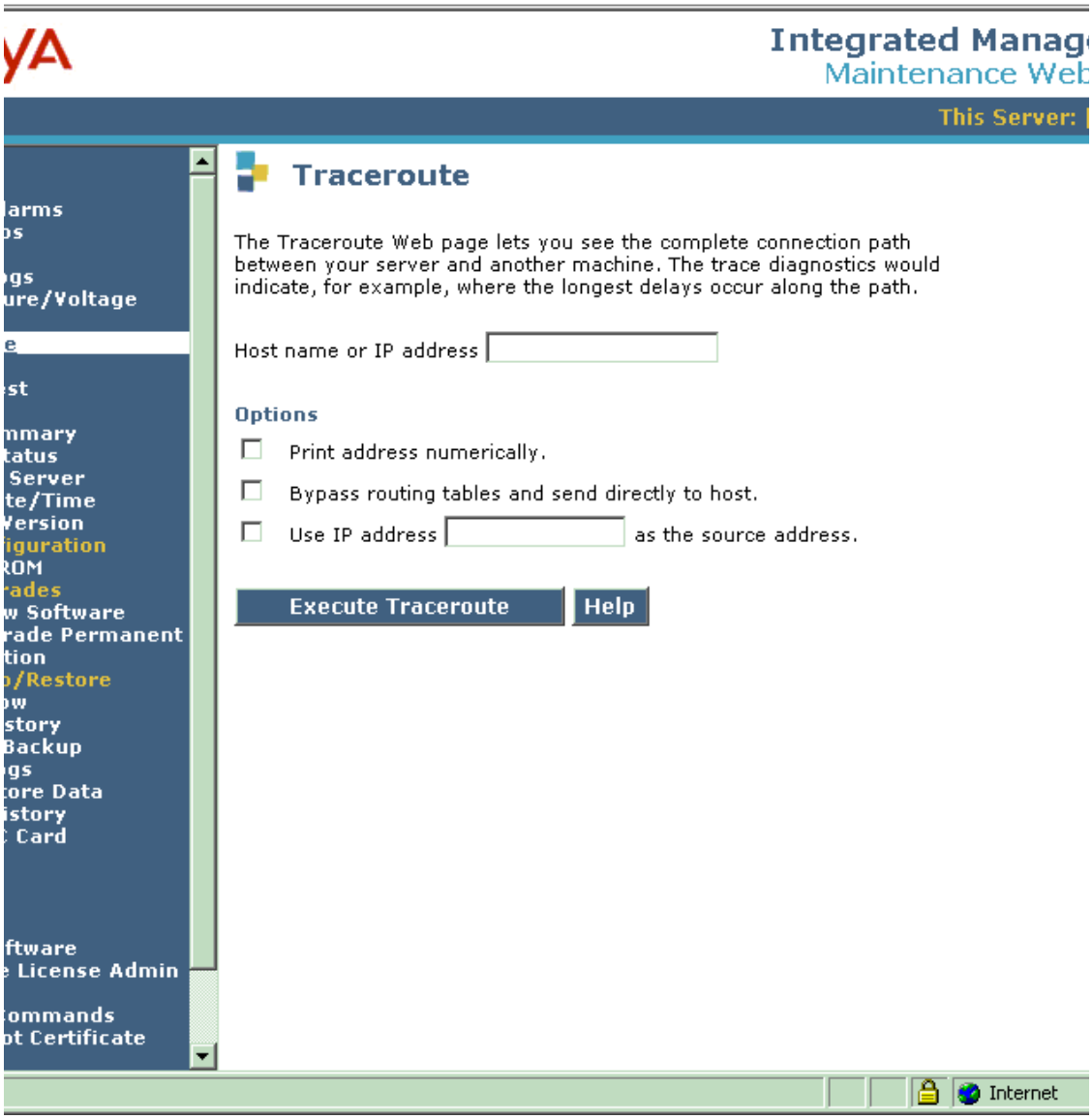
Packets are rejected. This message indicates that the host is rejecting the packets.

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.



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.

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 INode

/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 is 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 140.

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 page to test your modem and ensure it is working properly. The modem is used to report 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.

Modem Test screen field descriptions

Test Options

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

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 active or standby 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 active or non-active.

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

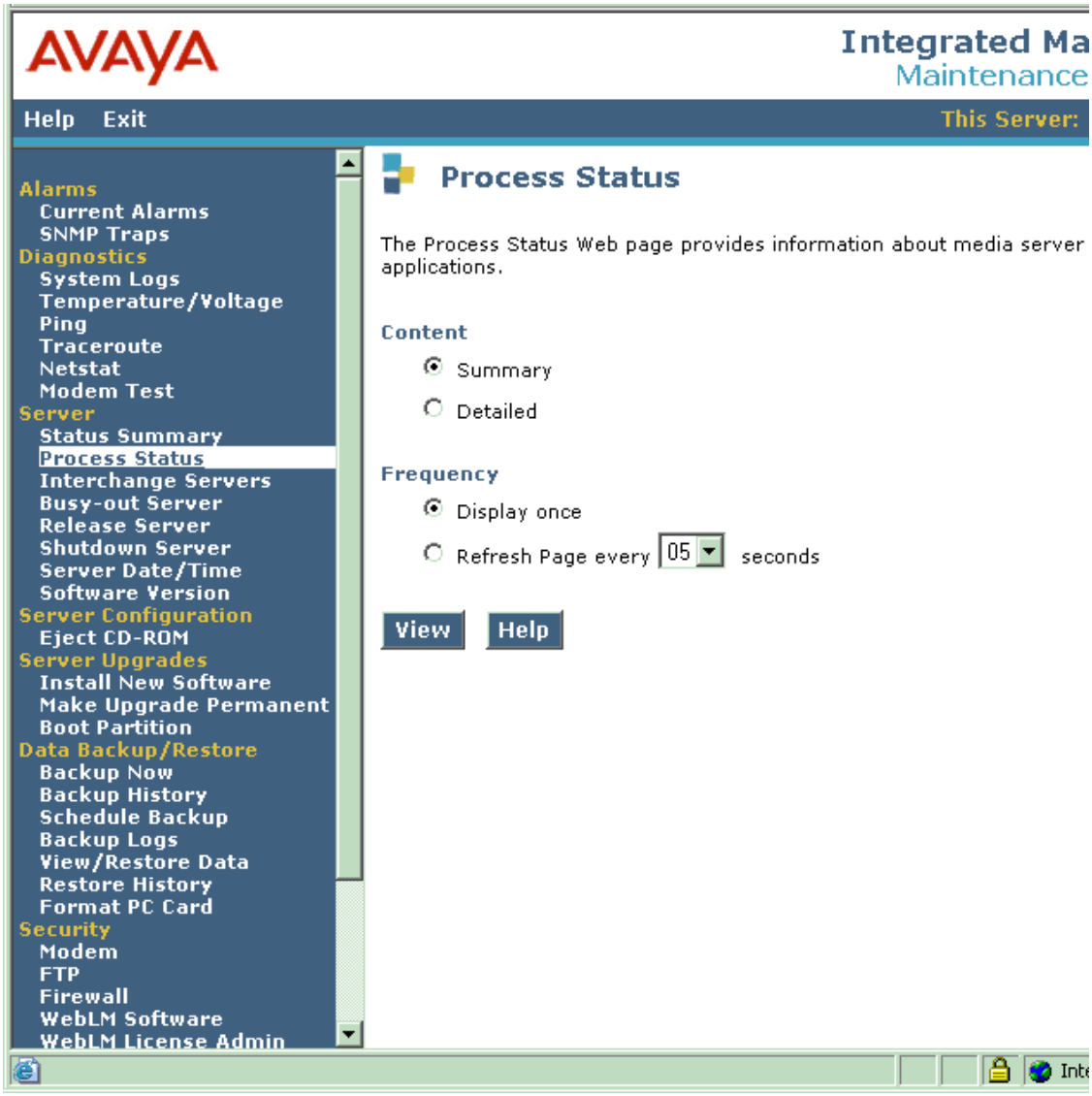
To view overall status information about the servers:

- 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 145.
- 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 **Refresh page repeatedly every __ seconds** 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.



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 __ 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.

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 146***: 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 Converged Communications Server write messages.
INADSAlarmAgent	Sends alarms to the Initialization and Administration System (INADS) using SNMP traps defined in the INADS Management Information Base (MIB).
CCSTrapAgent	Acts to send Simple Network Management Protocol (SNMP) traps defined for the Converged Communications Server.
GMM (Global Maintenance Manager)	Collects, processes, and reports system-wide alarms.

Application Name	Description
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 running on CCS 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 active 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 active or dormant. Also use this server page to safely bring down the server immediately or later on, and whether it reboots after the shutdown.

WARNING:

When you Shut down this server, the web server stops 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.

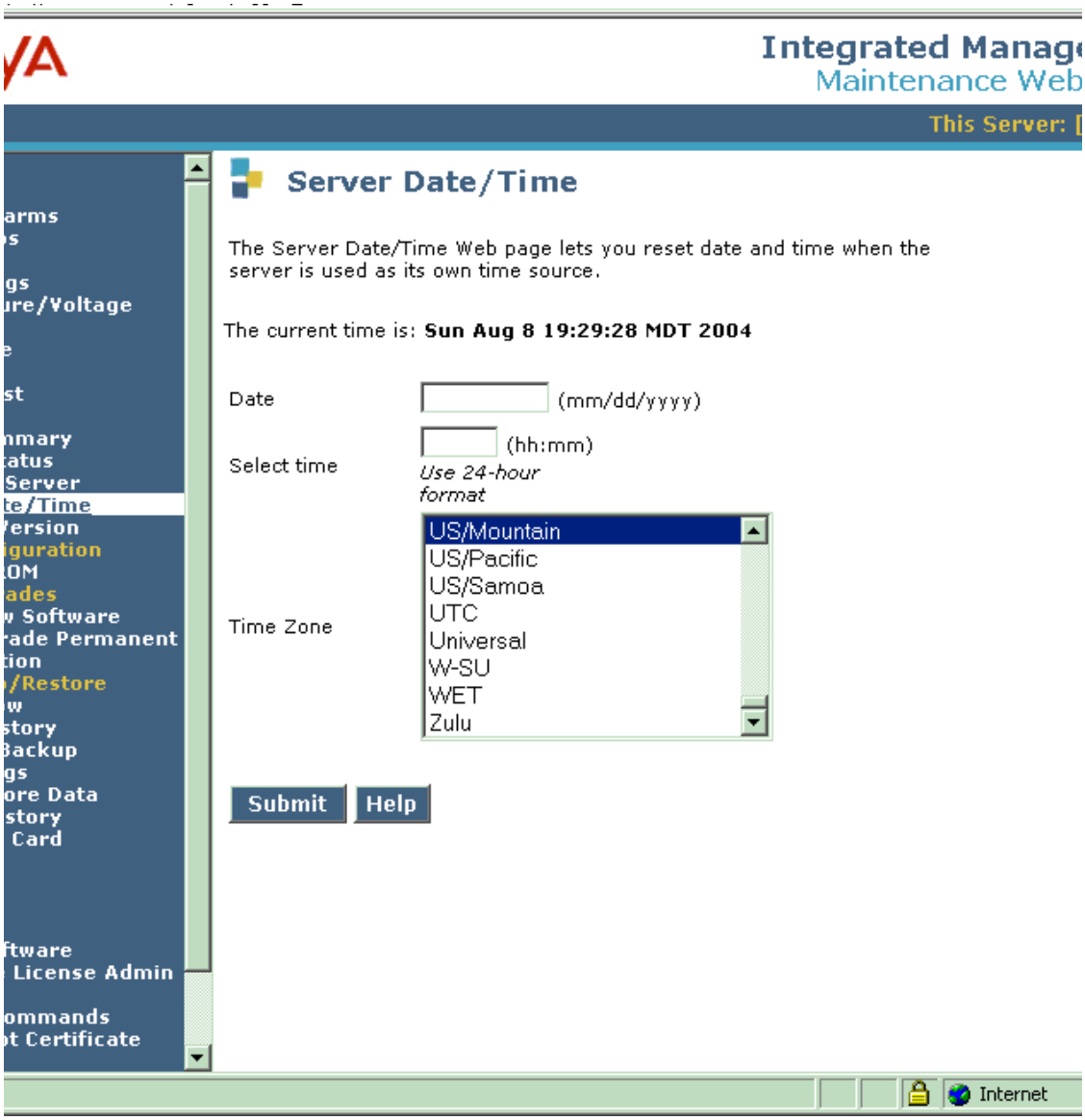
Restart Server after shutdown. Select this option to reboot after shutting down.

Shutdown even if this is the active server. Select this option if this server is the active 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.



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 as needed to adjust the time.
- If the Avaya server is synchronizing its time with a Network Time Server (NTS) external time source, you set the time using this page only during initial configuration in order 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.

The Avaya Converged Communications Server software relies on the time of day setting for many system functions, including:

- 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 current time is displayed 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 in order 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 will 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 be current or not current.

Select Time

Enter the hours and minutes.

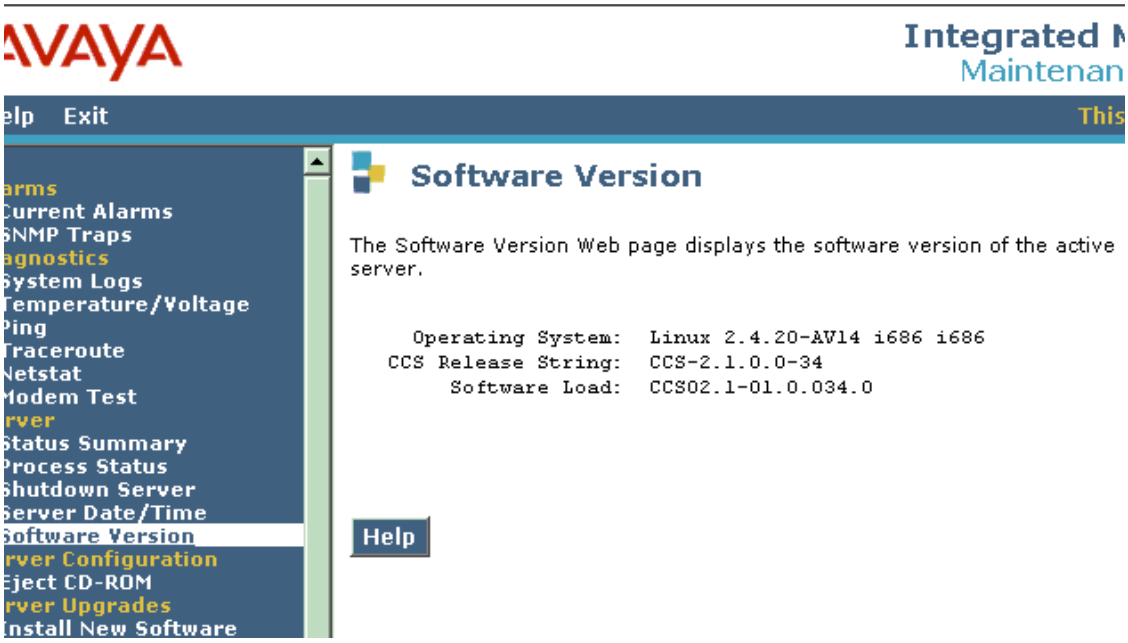
Time Zone

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 this Avaya server is running. You may want to check your software version before, during, or after you install new software.



Software Version screen field descriptions

Operating System

(Read-Only) The release and issue number of the Linux operating system that is running 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 Converged Communications Server software that is running on the server. For example:

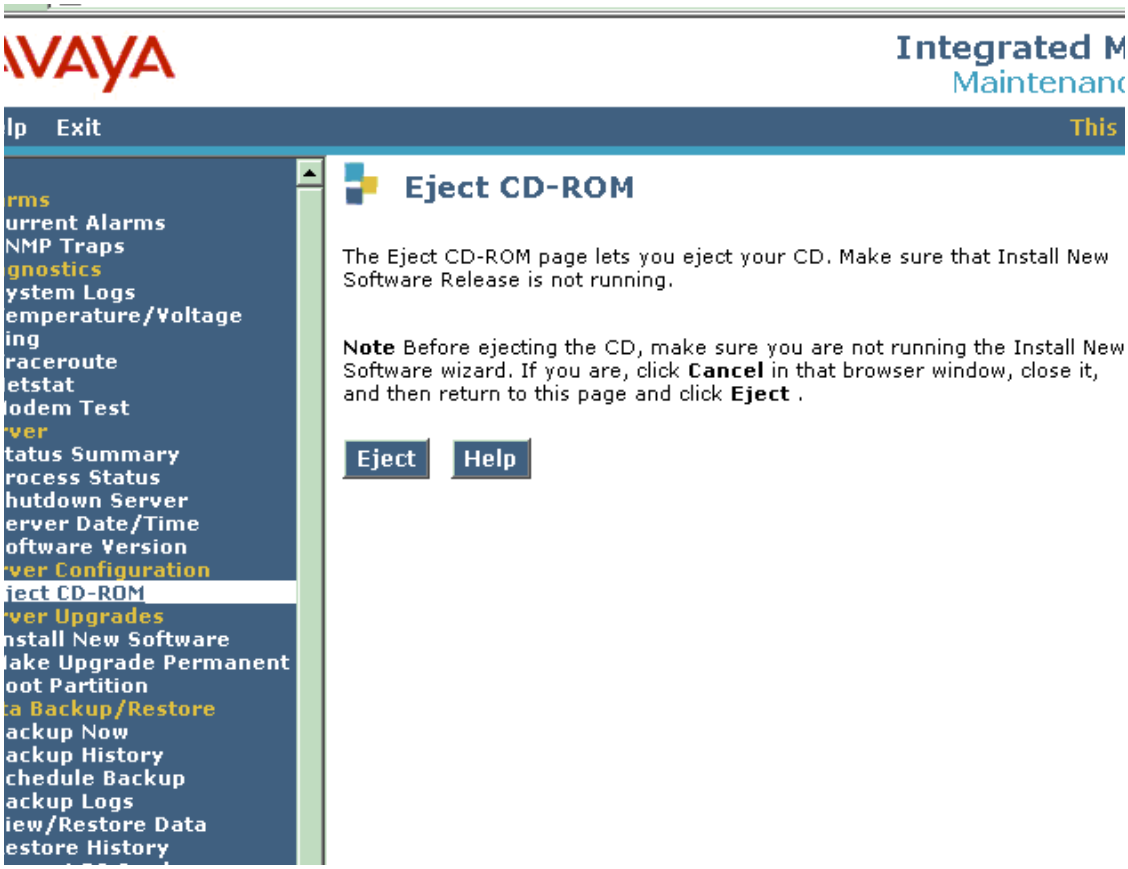
CCS-2.1.0.0-34 is the release (by field: major release, minor release, development release, Avaya build).

Software Load

The fuller version of the software release name. The major release, minor release, development release, subrelease, followed by the load number, such a 034, that is incremented for each new software build, and the final number: an additional release number, for internal use only.

Server Configuration

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 "Install New Software Release". 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

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 CCS02.1-01.0.032.0 in the FTP directory on the server's hard drive.

  NOTE:
  The software releases subdirectory on the server's hard drive (this contains the current software load that the server is running, and is used only to reinstall the current software version.

- Release CCS02.1-01.0.032.0 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

The License Source page allows the input of the correct license file and Avaya authentication file, which must be installed for the software to function.

- A new server requires the installation of both a license file and an Avaya authentication file.
- Subsequent upgrades may require installation of a license file only to authorize access to new features.

To indicate where to find the license and Avaya authentication files:

1. Click one of the following selections. These options may not appear on all systems:
   - ***Supply files when prompted***. Choose this option to copy the correct files to the active partition. You typically choose this option when upgrading software on the system's only server, or when upgrading the first of two duplicated servers.
   - ***Copy files from duplicated server***. If the duplicate server has the correct copy of the software license and Avaya authentication files, copy them to the server. Select this option if you already upgraded the duplicate server to run the new software, and are now upgrading the second server.
   - ***Reuse files on the active partition of this server***. Choose this option only if new license and authentication files are not needed for this software release (for example, if the software corrects problems without adding new features).
2. Click **Continue**.

Review Notices

What you need to know about the Install Software Wizard:

Install New Software wizard: Use to upgrade the version of software that the server is running. You access this wizard from the Web navigation panel -- **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 is 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 don't 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, it must be re-entered 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 step 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 don't 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 wascopied 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 active server and a standby 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 an active server warning. It is okay to proceed.

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 standby 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 active server and a standby 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 active server. The server that you arelogged into becomes the current standby server.
  - The current standby server is now busied out, then rebooted to install the new software.
  - If you are working on the standby server, call processing is normally unaffected during the 15 minutes that the server needs to reboot. If for some reason the active 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 active.

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 active 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 page is the last step required for completing the installation of a new software release. It sets up the server to reboot from the currently active (new) software version, instead of rebooting to the previous version.

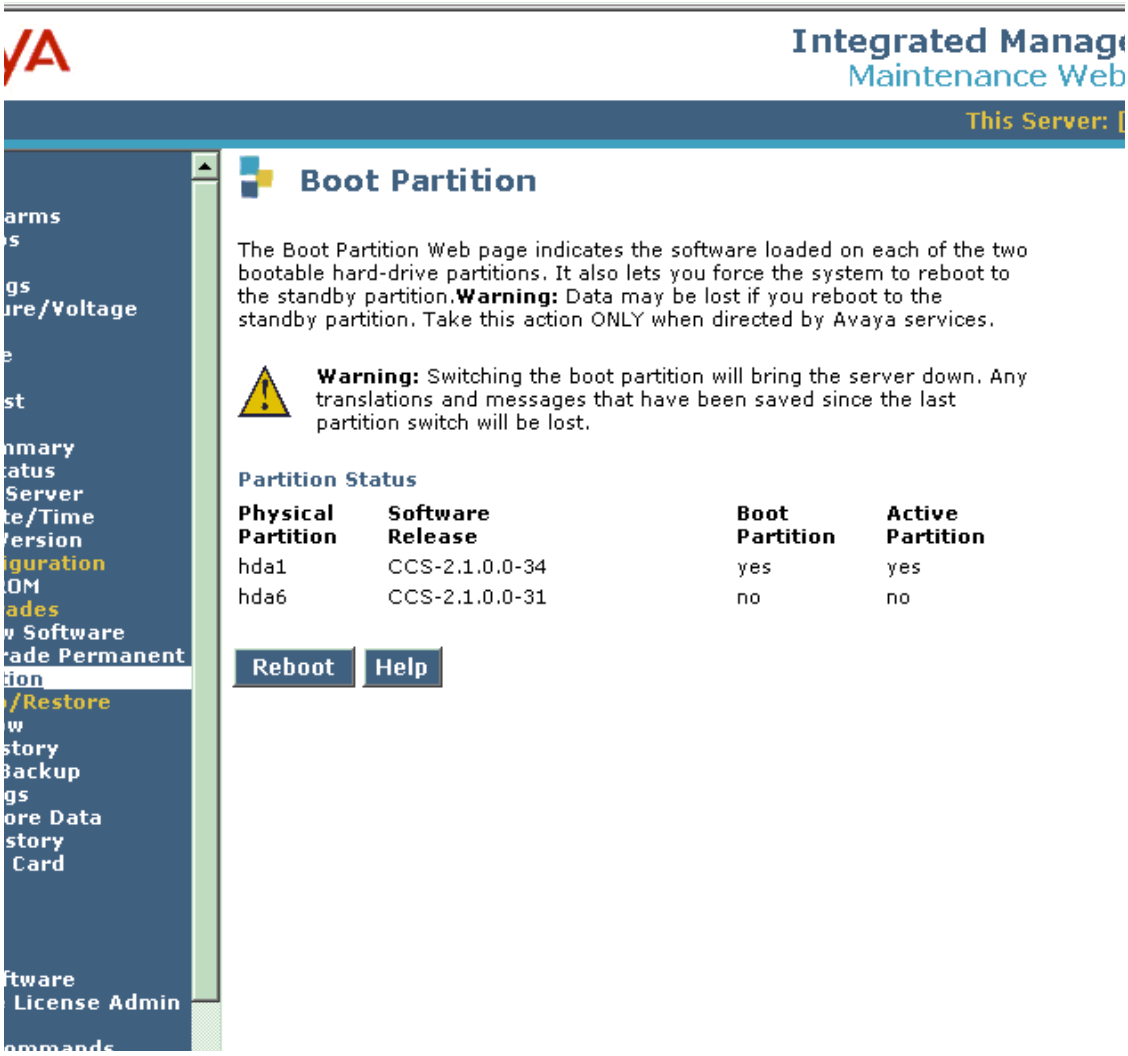
- You do not need to change the server status to standby.
- Because the Install New Software wizard must be run on each server to upgrade it, you need to use this page on each server after you complete a software installation.

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.


Integrated Manage
Maintenance Web
This Server: [
arms
s
gs
re/Voltage
st
mary
atus
Server
e/Time
ersion
guration
OM
ades
Software
ade Permanent
ion
/Restore
w
story
ackup
gs
ore Data
story
Card
tware
License Admin
ommands
t Certificate
Make Upgrade Permanent
The Make Upgrade Permanent Web page is used to make the most recent software upgrade permanent. This action is required following an upgrade. This prevents the server from rebooting to an older release.
WARNING: Clicking the Submit button will cause the disk boot partition to be set to the partition which is currently running. If the current partition is already the boot partition, this action has no effect.
Submit
Help
Internet

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. This will not affect service 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..

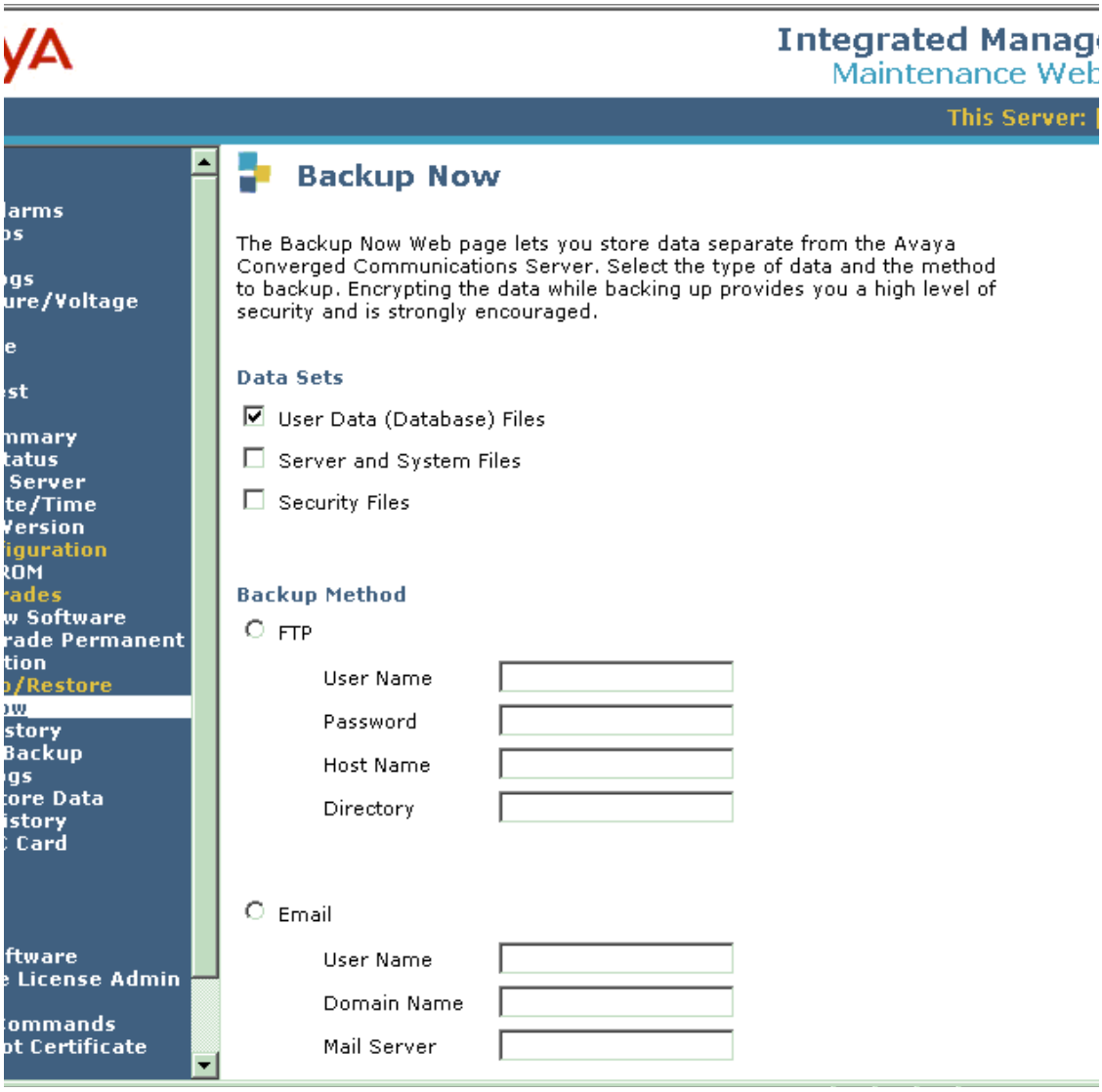
Partition	Software release	Reboot next from here	Currently active
1	Pre-upgrade version	no	no
6	New software version	yes	yes

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 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 is 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.
- **Email**. Choose this selection to send the backup data as an attachment to an email. 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 via email, 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 email 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 and therefore the backup process does not depend on other servers being available and accessible.
  - You can physically remove USB memory and place it in offsite storage for safekeeping.
  - However, flash memory has limited storage space. Also, if it is not sent offsite 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 179.

Encryption

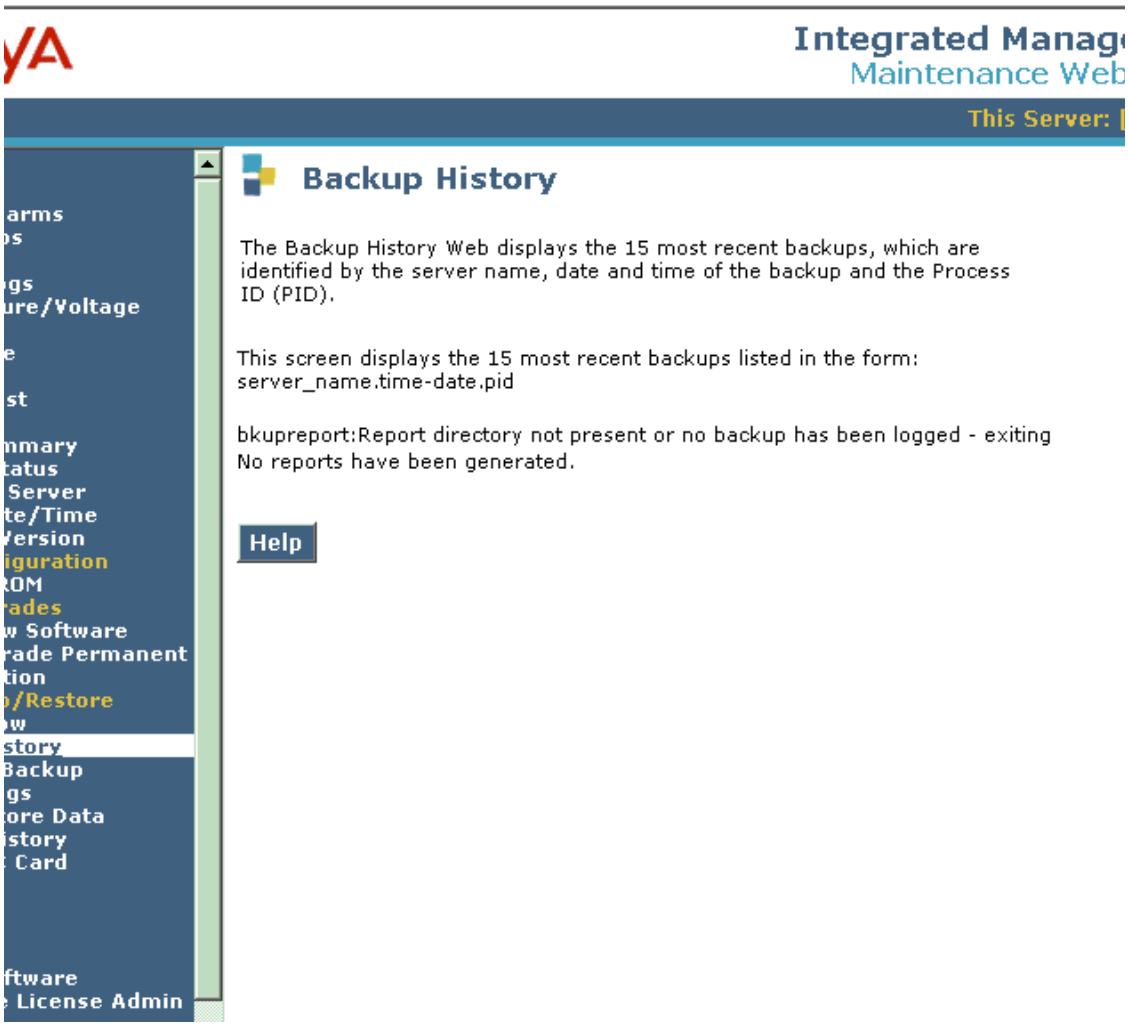
If you want to encrypt the backup data, click the box in the Encryption area of the page and enter a pass phrase using an arbitrary string of 15 to 256 characters. The pass phrase can contain any characters except the following (single quote, backslash, single backquote, quote, percent sign): **’ \ & ‘ " %**

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 page 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 backups (15).

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

Schedule Backup screen field descriptions

The backup procedure runs automatically, based on the schedule you create. Use the Schedule Backup page 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 is 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 was recorded. It corresponds to the backup method used for the backup. Possible destinations are: FTP, email, and local PC card.

Add a backup schedule

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 datasets 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 2 copies of all datasets 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.

1. On the Schedule Backup page, click 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 page displays the information for the backup schedule you selected in step 2.
3. Make the changes you want to the backup schedule.
4. For detailed information about data sets, backup method, encryption, and timing for the backup schedule, see Backup strategies.
5. 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

Backup Logs screen field descriptions

When you back up data, the system creates an image as a "tar" file that contains information, such as what data sets were backed up, whether or not the backup was successful, and how the data was 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 was 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 was recorded. It corresponds to the backup method used for the backup. Possible destinations are: FTP, email, and local PC card.

Steps to preview or restore backup data

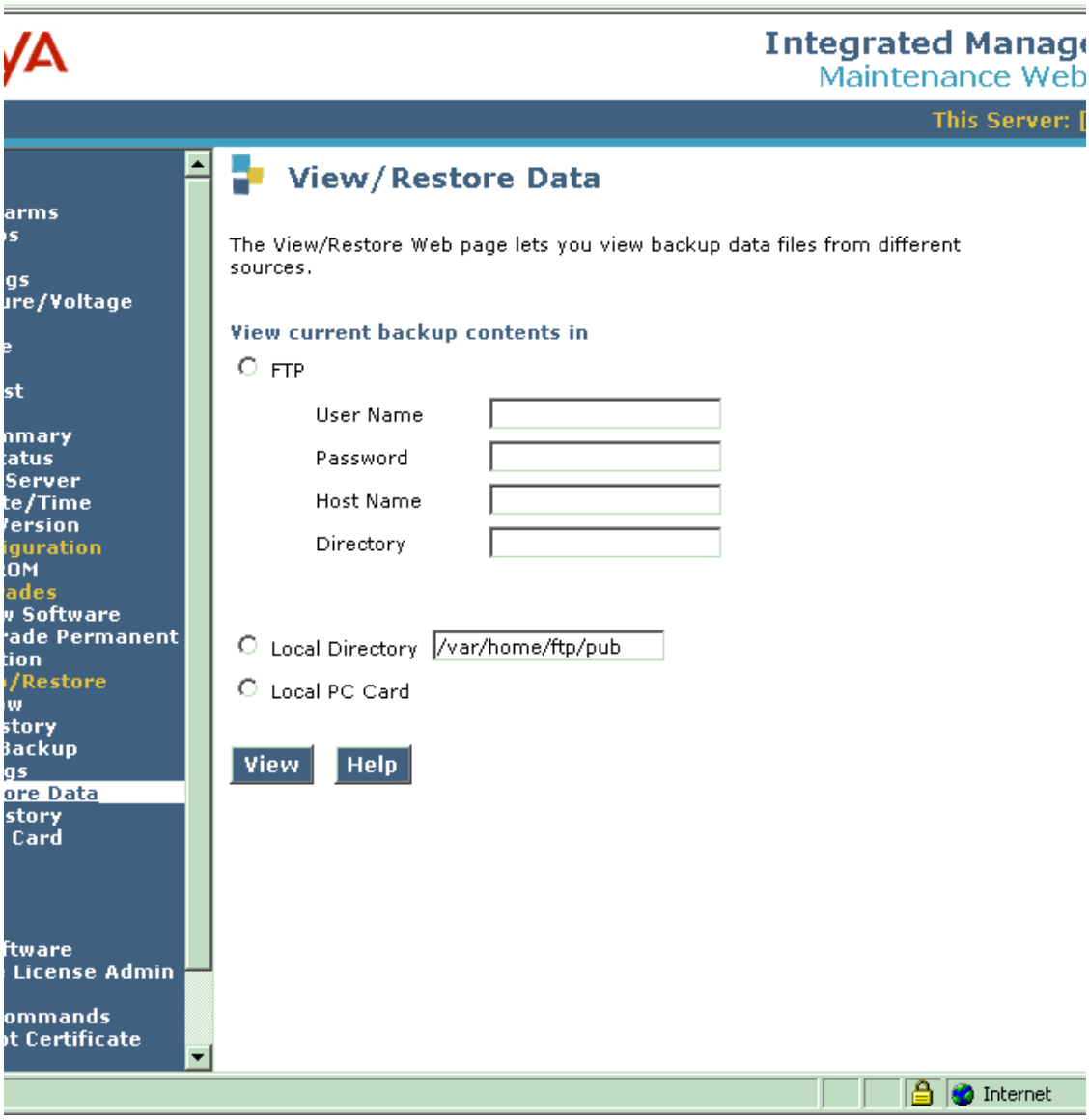
Click one of the following buttons:

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 was backed up via email, or if the data was backed up via FTP but the FTP server does not allow reading, the file to be restored must first be copied to this server via FTP or via an download function. Once the file is copied to this server, it can be restored.

View/Restore Data screen



View/Restore Data screen field descriptions

If your system malfunctions and you lose data, this saved data from the backup can restart the system. Copy the data to the server from the location it was saved. Restore a backup image, which is a "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 "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 email 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 was 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 is 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 memoy 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 offsite storage safekeeping.
- However, flash memory has limited storage space. Also, if it is not sent offsite 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

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:

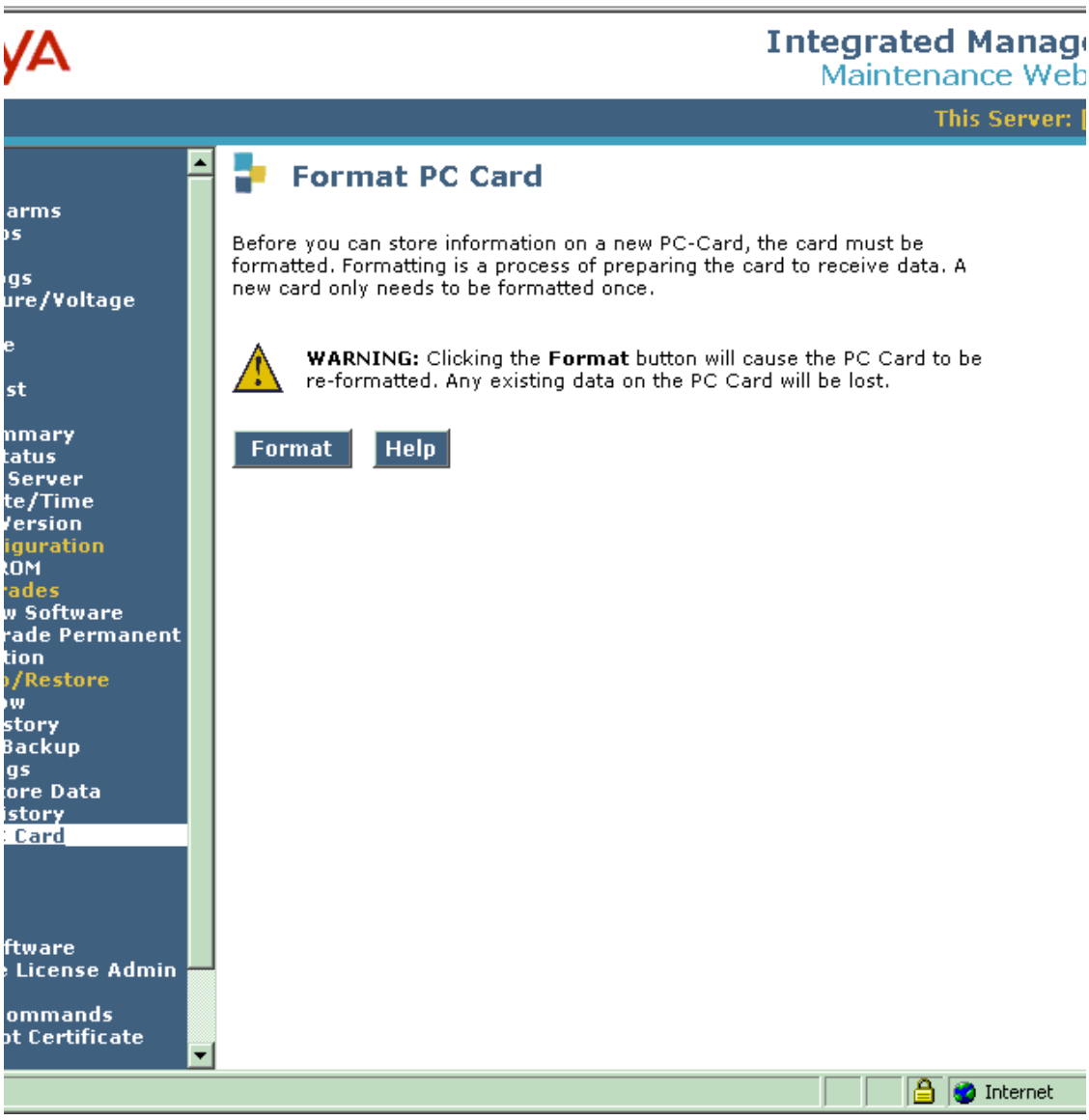
1 lzccs1.163608-20040719.5179

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 amy also format the flash memory in conjunction with the Backup Now screen on page 167.



Format PC Card results screen

The results of your PC card format displays.

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.

Modem screen field descriptions

Modem Administration

To check or change the call-receiving status of this server's modem:

- **Disable**. 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

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 step 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.

Steps 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 email 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 checkbox 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 corporate 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 email 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 "put" to 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.

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 "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.


Integrated Manag
Maintenance Web
This Server:
The Firewall Web page lets you enable network services on the corporate LAN interface to the Avaya media server. Unselected services are automatically disabled.
WARNING: Some network services are required for proper operation of or access to the server.For additional details, click Help.
Please wait...
Input to Server
Output from Server
Service
Port/Protocol
ftp-data 20/tcp
ftp 21/tcp
ssh 22/tcp
telnet 23/tcp
smtp 25/tcp
domain 53/tcp
domain 53/udp
ntp 123/udp
https 443/tcp
def-sat 5023/tcp
ping echo-request/icmp
Submit
Advanced Setting...
Help
Internet

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 (checkbox 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 email 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 Avaya 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 checkbox 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.

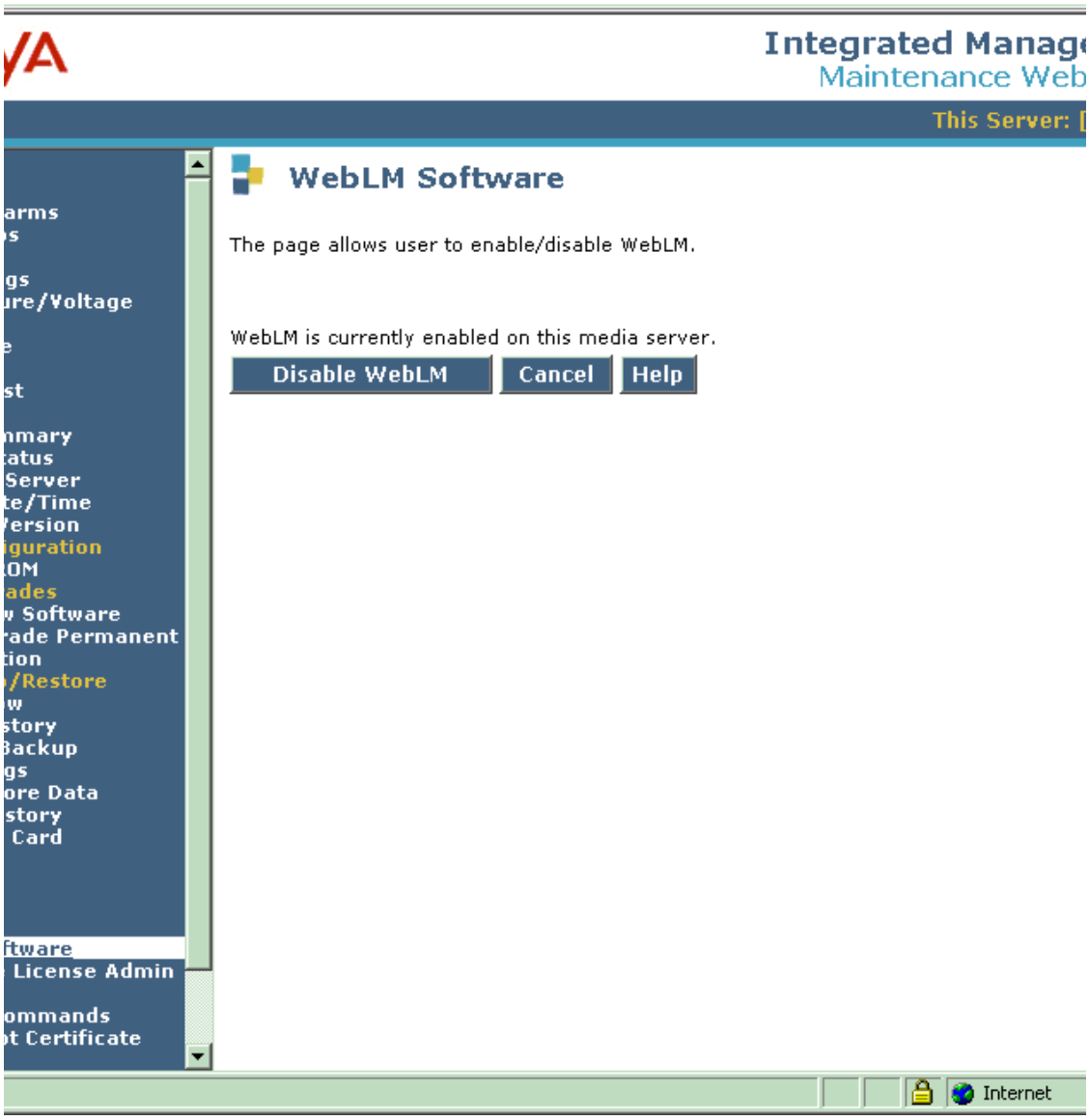
- To view all IP services:

  Click Advanced Setting to adjust the status of a service that is not listed on the first page. This page redisplays, 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/disable it.



WebLM Software screen field descriptions

You have the flexibility to manage features and capacities among all CCS 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.

NOTE:
The license expiration date is verified when installing WebLM software. The date generated by 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.)

How the WebLM License File Works

- WebLM obtains the host ID (MAC address) of the machine from which it runs.
- It then initiates an HTTPS connection directly to the RFA server, and sends a POST request with the SAP order number and the host ID.
- The RFA sends the license file that is digitally signed using the host ID as part of the key.
- After the license file is generated, RFA sends the file contents as a POST reply to WebLM which saves the file and updates the internal license data of the product.

WebLM License Admin screen

WebLM License Admin field descriptions

Select **Access WebLM** to view the WebLM application.

WebLM License File

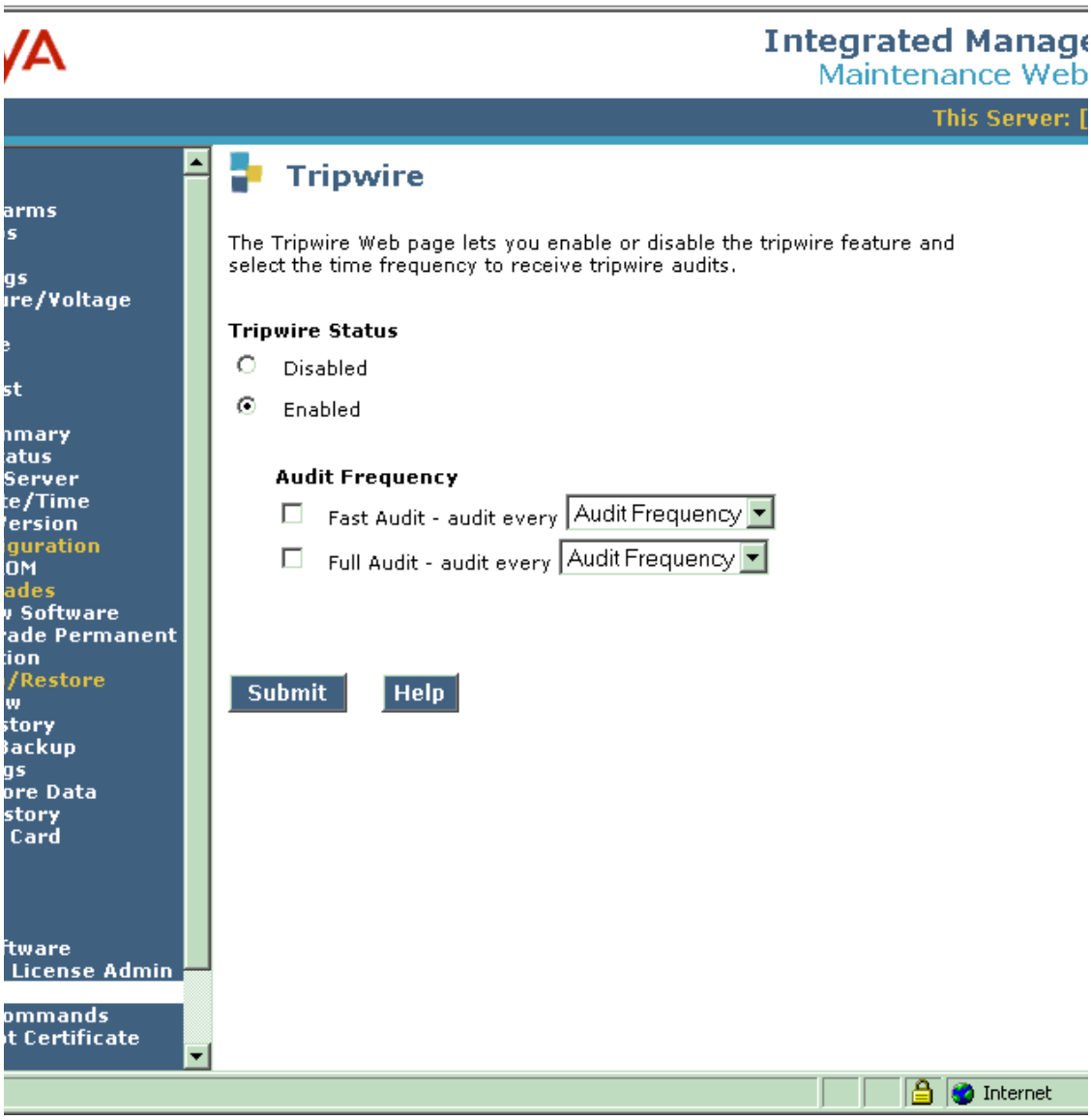
WebLM is a tool that enforces and defines the capacity limits of an Avaya server to the license file, which is generated by the Remote Feature Activation (RFA). The capacity limits are then allocated to the individual Avaya servers using license files.

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 CCS 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



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 and .-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 butstarts at the next time interval you specify.). 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.

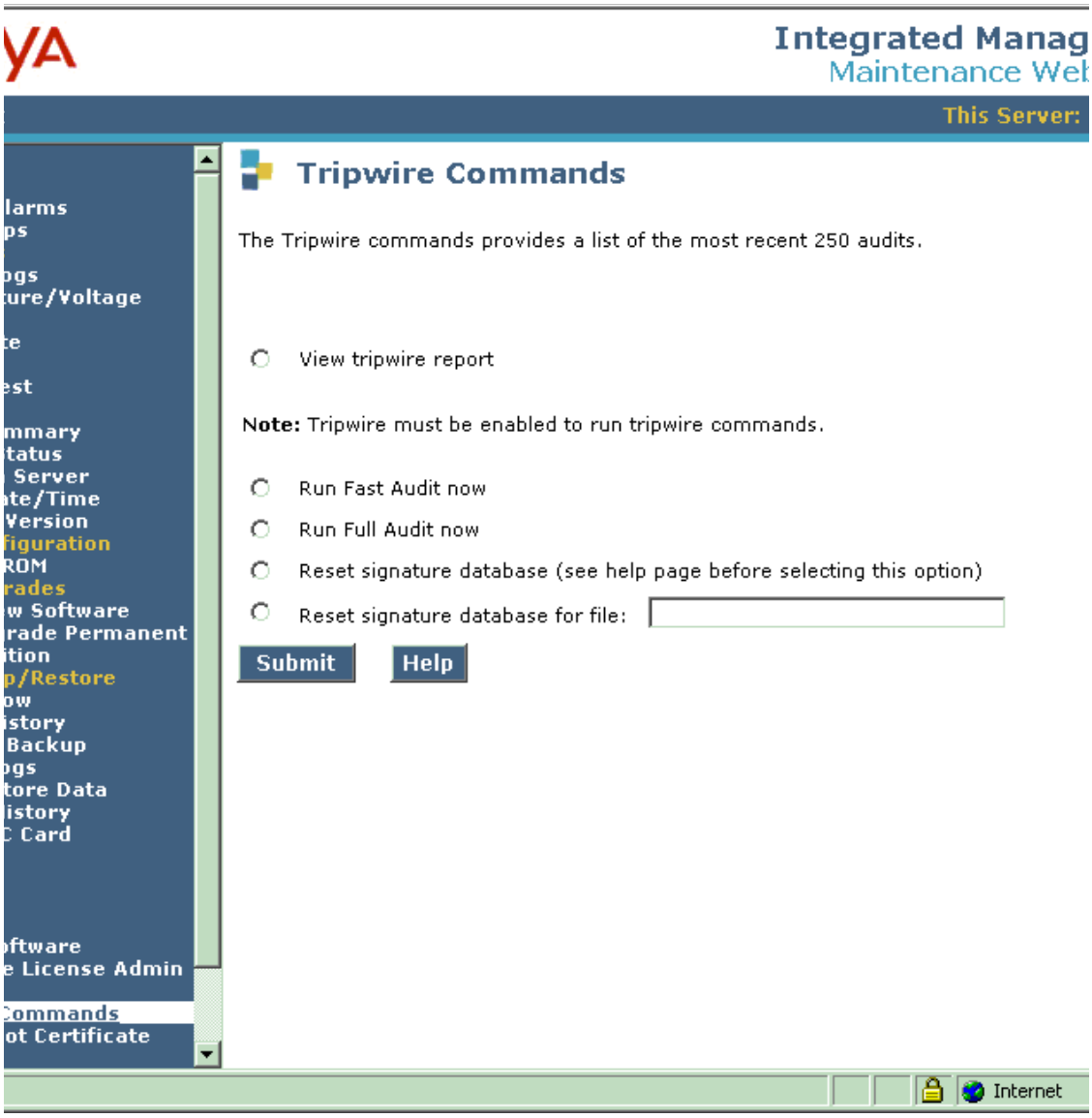
Full Audit

The standard times are:

- hourly jobs: one minute past the hour, as in 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



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**.

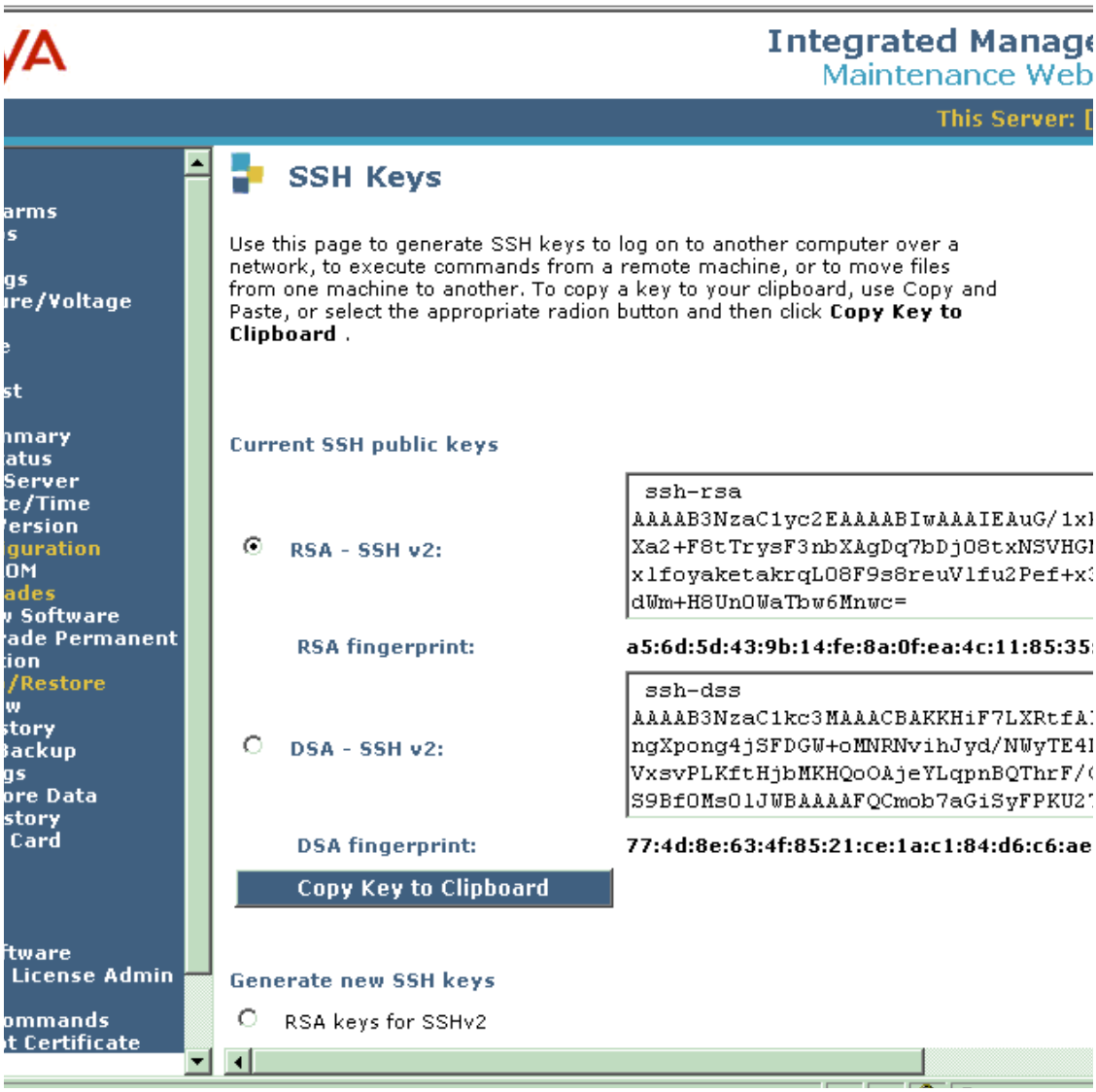
Install Root Certificate screen

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

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.

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; therefore 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.

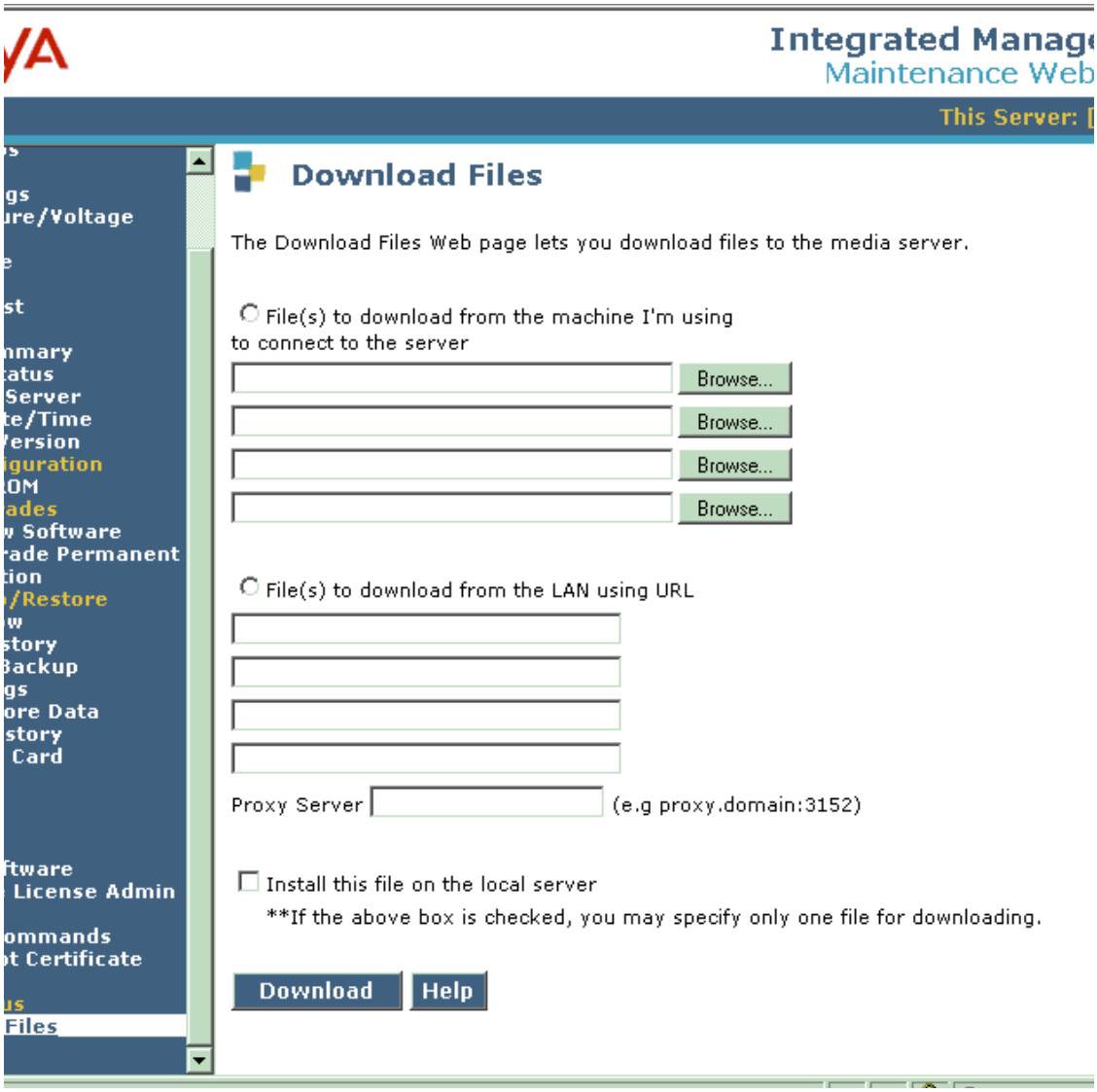
- RSA keys for SSHv2
- DSA keys for SSHv2

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.



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: Licenses

Major applications

Each of the major components has its own license, which is included blow.

Red Hat 8	Red Hat License
Postgres	Berkeley License
Apache	Apache License
Xerces	Apache License
Ace	ACE License
Hughes SDF	Not open source – licensed from Hughes
Perl	Artistic License
Php	PHP License 3.0 -- attached
Pear	Individual licenses – see next table
Smarty	LGPL
Ismo	LGPL

PEAR Packages

PEAR packages are individually licensed by their contributors. These are summarized below.

PEAR Core packages	2.02 PHP License
Config	2.02 PHP License
Validate	2.02 PHP License
XML/Tree	2.02 PHP License
Crypt/Xtea	2.02 PHP License
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 License

```
-------------------------------------------------------------------
                  The PHP License, version 2.02
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.

1. 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.
2. 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.

3. 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:
    a. 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.
    b. use the modified Package only within your corporation or organization.
    c. 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.
    d. make other distribution arrangements with the Copyright Holder.
4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:
    a. 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.
    b. accompany the distribution with the machine-readable source of the Package with your modifications.
    c. 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.
    d. make other distribution arrangements with the Copyright Holder.
5. 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.
6. 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.

7. 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.
8. 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.
9. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.
10. 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 supercede, 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(TM) and TAO(TM)

ACE(TM) and TAO(TM) 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, noninfringement, 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(TM), TAO(TM), 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(TM) or TAO(TM), 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.

Glossary

A

access code
A dial code of 1 digit to 3 digits that is used to activate a feature, cancel a feature, or access an outgoing trunk.

Access Security Gateway (ASG)
An optional interface that can be used to secure the administration and maintenance ports on the system.

Active
In a duplex configuration supporting local failover, this is the server which is running the SIP applications and services. Sometimes referred to as the primary. Compare with Standby.

American National Standards Institute (ANSI)
A professional technical association that supports standards for transmission, protocol, and high-level languages, and that represents the US in the International Organization for Standards. ANSI standards are for voluntary use in the US.

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

bearer channel (B-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 data channel (D-channel).

bus
A multiconductor electrical path that is used to transfer information over a common connection from any of several sources to any of several destinations. *See also* packet bus; time-division multiplex (TDM) bus.

C

Call Detail Recording (CDR)
A file that uses software and hardware to record call data. CDR was formerly called Station Message Detail Recording (SMDR). *See also* Call Detail Recording utility (CDRU).

Call Detail Recording utility (CDRU)
Software that collects, stores, filters, and provides output of call detail records. *See also* Call Detail Recording (CDR).

carrier
An enclosed shelf that contains vertical slots that hold circuit packs.

central office (CO)
Telephone switching equipment that provides local telephone service and access to toll facilities for long distance calling.

channel
(1) A circuit-switched call. (2) A communications path that is used to transmit voice and data. (3) In WebLM transmission, all the contiguous time slots or noncontiguous 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* data channel (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.

Class of Restriction (COR)
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* Class of Service (COS).

Class of Service (COS)
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* Class of Restriction (COR).

CCITT
Comitte Consultatif International Telephonique et Telegraphique. *See* International Telecommunications Union (ITU).

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 Point-to-Point Protocol (PPP)s. *See also* SSH.

Controlled Local Area Network (CLAN) circuit pack
A circuit pack (TN799B) in an Avaya DEFINITY port network (PN) that provides TCP/IP connectivity to adjuncts over Ethernet or Point-to-Point Protocol (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.

Converged Communications Server (CCS)
Avaya's proxy server for Session Initiation Protocol (SIP), supporting instant messaging using the client in Avaya IP Softphone R5 or later, and voice communication using Avaya 4602SIP phones.

CPN
called-party number

CPN/BN
calling-party number/billing number

customer-premises equipment (CPE)
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

data channel (D-channel)
A 16-kbps channel or a 64-kbps channel that carries signaling information or data on an Integrated Services Digital Network Basic Rate Interface (ISDN-BRI) or Integrated Services Digital Network Primary Rate Interface (ISDN-PRI). *See also* bearer channel (B-channel); data channel (D-channel).

data communications equipment (DCE)
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 packet assembly/disassembly (PAD).

data module
An interconnection device between a Basic Rate Interface (BRI) or a Digital Communications Protocol (DCP) interface of the SSH, and the data terminal equipment (DTE) or data channel (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.

data terminal equipment (DTE)
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.

digital
The representation of information by discrete steps. Compare with *analog*.

Digital Communications Protocol (DCP)
A proprietary protocol that is used to transmit 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.

DIMM
Dual Inline Memory Module

dual-tone multifrequency (DTMF)
The touchtone signals that are used for in-band telephone signaling.

duplex
The CCS host configuration supporting local failover via the interchange of the Active and Standby servers. Any one CCS host node may comprise two interconnected servers. Compare with simplex.

Dynamic Host Configuration Protocol (DHCP)
An IETF protocol (RFCs 951, 1534, 1542, 2131, and 2132) that assigns IP addresses dynamically from a pool of addresses instead of statically.

E

Edge
In Avaya's SIP architecture, this is the proxy server that forwards requests to/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 is used to route calls through a communications system. With a Uniform Dial Plan (UDP) or a main-satellite dialing plan, extensions are also used to route calls through a Point-to-Point Protocol (PPP).

F

FTP

File Transfer Protocol..

H

H.323

An International Telecommunications Union (ITU) standard for switched multimedia communication between a LAN-based multimedia endpoint and a gatekeeper. *See also* Session Initiation Protocol (SIP).

Home

This is the domain providing service to a SIP user, used in registering that user with a Home proxy.

host computer

A computer that is connected to a network, and that processes data from data-entry devices.

I

IE

See information element (IE).

IEEE

See Institute of Electrical and Electronics Engineers (IEEE).

IETF

See Internet Engineering Task Force (IETF).

IM

Instant Messaging. The instant-messaging client software required for Release 2.x or later of Avaya Converged Communications Server (CCS) is a version of the Avaya IP Softphone R5 or later.

information element (IE)

The name for the data fields within an Integrated Services Digital Network (ISDN) Layer 3 message.

Institute of Electrical and Electronics Engineers (IEEE)

An organization that, among other things, produces standards for local area network (LAN) equipment.

Integrated Services Digital Network (ISDN)

A public network or a Point-to-Point Protocol (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* Integrated Services Digital Network Basic Rate Interface (ISDN-BRI); Integrated Services Digital Network Primary Rate Interface (ISDN-PRI).

Integrated Services Digital Network Basic Rate Interface (ISDN-BRI)

The interface between a communications system and terminal that includes two 64-kbps bearer channel (B-channel)s for transmitting voice or data, and one 16-kbps data channel (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* Integrated Services Digital Network Primary Rate Interface (ISDN-PRI).

Integrated Services Digital Network Primary Rate Interface (ISDN-PRI)

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 bearer channel (B-channel)s for transmitting voice and data, and one 64-kbps data channel (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* Integrated Services Digital Network (ISDN); Integrated Services Digital Network Basic Rate Interface (ISDN-BRI).

interchange

Term used for when the Active server in a duplex configuration relinquishes control and its Standby server takes over that control, running the SIP software applications and services for this CCS node.

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 American National Standards Institute (ANSI).

International Telecommunications Union (ITU)

An international organization that sets universal standards for data communications, including Integrated Services Digital Network (ISDN). ITU was formerly known as International Telegraph and Telephone Consultative Committee (CCITT).

International Telegraph and Telephone Consultative Committee

See International Telecommunications Union (ITU).

Internet Engineering Task Force (IETF)

One of two technical working bodies of the Internet Activities Board. The IETF develops new Transmission Control Protocol (TCP)/Internet Protocol (IP) (i.e., TCP/IP) standards for the Internet.

Internet Protocol (IP)

A connectionless protocol that operates at Layer 3 of the Open Systems Interconnect (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 Transmission Control Protocol (TCP), and is usually identified as TCP/IP.

L

local area network (LAN)

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 in CCS R2.1 and later that supports database replication and interchange, as needed, between two servers (one Active, one Standby), which are connected in a duplex configuration.

M

MAC address (or MAC name)
A 48-bit number, uniquely identifying and programmed into each network interface card or device.

Management Information Base (MIB)
A directory listing logical names of resources on a network, perinent 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.

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

Off-Premises Station (OPS)
A telephone that Avaya Communication Manager does not control, such as a cellular telephone or the home telephone of a user. The features of Communication Manager can be extended to an OPS through switch administration by associating the extension of the office telephone with the off-site telephone. NOTE: Session Initiation Protocol (SIP) endpoints are administered on Communication Manager as OPS.

Open Systems Interconnect (OSI)
A system of seven independent communication protocols defined by the International Organization for Standards or ISO. Each of the seven layers 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.

O/S
Operating System.

P

packet
A group of bits that is used in packet switching and that is 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.

packet assembly/disassembly (PAD)
The process of packetizing control data and user data from a transmitting device before the data is forwarded through the packet network.The receiving device disassembles the packets, removes the control data, and then reassembles the packets, thus reconstituting the user data in its 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 *packets*. 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.

Plain Old Telephone Service (POTS)
Basic voice communications with standard, single-line phones accessing the public switched telephone network (PSTN).

Point-to-Point Protocol (PPP)
A standard (largely replacing 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
Another name for the Active server, or server A, running the SIP applications and/or proxy services in a duplex configuration. Compare with secondary.

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 will interpret and forward requests intended for specific users to their particular Home proxy servers.

public network
A network to which all customers have open access for local calling and long distance calling.

public switched telephone network (PSTN)
The public worldwide voice telephone network.

R

RAS
Remote Access Server (or in Microsoft Windows opearting systems, Remote Access Service).

Real Time Transfer Protocol (RTP)
An Internet Engineering Task Force (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 local area network (LAN) that is designed for data. RTP gives higher priority to video and other real-time interactive exchanges than to connectionless data.

RFA
Remote Feature Activation is a web-based application which is used to obtain 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

RTC
Real Time Communication

RTCP
Real Time Control Protocol

S

secondary
Another name for the Standby server, or server B, in a duplex configuration. Compare with primary.

Session Initiation Protocol (SIP)
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; Voice over IP (VoIP).

simplex
The standard CCS host configuration with one server/database per node. Compare with duplex.

SSH
Secure SHell is a protocol for secure remote login and other secure network services over an insecure network. It provides for server authentication, and data integrity with perfect port-forwarding secrecy.

Standby
In a duplex configuration supporting local failover, this is the server which is synchronized and ready to interchange with the Active server. Sometimes referred to as the secondary.

subscriber
A Session Initiation Protocol (SIP) "subscriber" is one of the following: a Converged Communications Server (CCS) Release 2.1 host or other SIP node, a SIP user (per Contact), or a Media Server (running Avaya Communication Manager 2.1.1 or later for CCS 2.1).

switch
Any kind of telephone switching system. *See also* communications system.

T

TCP
See Transmission Control Protocol (TCP).

TCP/IP
See Internet Protocol (IP). *See also* Transmission Control Protocol (TCP).

tie trunk
A telecommunications channel that directly connects two private switching systems.

time-division multiplex (TDM) bus
A bus that is time-shared regularly by preallocating short time slots to each transmitter. In a SSH, all Plain Old Telephone Service (POTS) circuits are connected to the time-division multiplex (TDM) bus, and any port can send a signal to any other port. *See also* time-division multiplexing (TDM).

time-division multiplexing (TDM)
A form of nultiplexing that divides a transmission channel into successive time slots. *See also* time-division multiplex (TDM) bus.

time slot
In the SSH, a time slot refers to either a digital signal level-0 (DS0) on a T1 facility or an E1 facility, or a 64-kbps unit on the time-division multiplex (TDM) bus or fiber connection between port networks (PNs) that is structured as 8 bits every 125 microseconds.

Transmission Control Protocol (TCP)
A connection-oriented transport-layer protocol, IETF STD 7. RFC 793, that governs the exchange of sequential data. Whereas the Internet Protocol (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.

Transport Layer Security (TLS)
An IETF standard (RFC 2246) to supercede Netscapes' Secure Socket Layer (SSL) and provide host-to-host data connections with encryption and certification at the transport layer, as the name implies.

trunk
A dedicated communications channel between two communications systems or central office (CO)s.

trunk access code (TAC)
A dial access code used to access a specific trunk.

trunk group
Telecommunications channels that are assigned as a group for certain functions, and that can be used interchangeably between two communications systems or central office (CO)s.

U

UDP
(1) User Datagram Protocol (UDP); (2) Uniform Dial Plan.

universal serial bus (USB)
A high-speed serial interface that is used primarily to add a printer, a modem, a keyboard, a mouse, or another peripheral device to a personal computer.

Uniform Resource Identifiers (URI)
URIs (a.k.a. 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 addressable (requestable) in the same, relatively simple way.

User Datagram Protocol (UDP)
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.

V

Voice over IP (VoIP)

A set of facilities that use the Internet Protocol (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 public switched telephone network (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 which 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

P

R

S

T

U

V

W