Avaya Aura™ Communication Manager Security Design

Release 6.0

03-601973
Issue 4
June 2010

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya.

End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya 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 to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by the said Avaya reseller and not by Avaya.

Licenses

The software license terms available on the Avaya Web site, http://support.avaya.com/licenseinfo/ are applicable to anyone who downloads, uses and/or installs Avaya software, purchased from Avaya Inc., any Avaya affiliate, or an authorized Avaya reseller (as applicable) under a commercial agreement with Avaya or an authorized Avaya reseller. Unless otherwise agreed to by Avaya in writing, Avaya does not extend this license if the software was obtained from anyone other than Avaya, an Avaya affiliate or an Avaya authorized reseller, and Avaya reserves the right to take legal action against you and anyone else using or selling the software without a license. By installing, downloading or using the software, or authorizing others to do so, you, on behalf of yourself and the entity for whom you are installing, downloading or using the software (hereinafter referred to interchangeably as "you" and "end user"), agree to these terms and conditions and create a binding contract between you and Avaya Inc. Or the applicable Avaya affiliate ("Avaya").

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

- Designated System(s) License (DS):
  End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- Concurrent User License (CU):
  End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.
- Named User License (NU):
  End User may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User" means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (for example, webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR):
  Customer may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License"). (See Third-party Components for more information).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

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 can 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, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site:

http://www.support.avaya.com/.

Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to:securityalerts@avaya.com.

Trademarks

Avaya® and Avaya Aura™ are trademarks of Avaya Inc.

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

All non-Avaya trademarks are the property of their respective owners.

Downloading documents

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

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support.

Contents

Chapter 1: Introduction

Information classifications and NDA requirements

This book provides security-related information divided into four Avaya identified information classifications. Table 1: Avaya information classifications on page 13 lists and describes the four Avaya information classifications.

Table 1: Avaya information classifications

Classification	Description
Avaya Restricted	This classification is for extremely sensitive business information, intended strictly for use within Avaya. Unauthorized disclosure of this information can have a severe adverse impact on Avaya, its customers, BusinessPartners, and suppliers.
Avaya Confidential	This classification applies to less sensitive business information intended for use within Avaya. Unauthorized disclosure of this information can have significant adverse impact on Avaya, its customers, BusinessPartners, and suppliers. Information that some people would consider private is included in this classification.
Avaya Proprietary	This classification applies to all other information that does not clearly fit into the two above classifications, and is considered sensitive only outside of Avaya. While disclosure might not have a serious adverse impact on Avaya, its customers, BusinessPartners, and suppliers, this information belongs to Avaya, and unauthorized disclosure is against Avaya policy.
Public	This classification applies to information explicitly approved by Avaya management as nonsensitive information available for external release.

The information herein is considered confidential and should not be shared outside of your organization or posted on any public web site. While there are references to additional information sources throughout the book, some sources disclose both confidential and proprietary information and require a non-disclosure agreement (NDA) with Avaya.

Disclaimer

Avaya has made reasonable commercial efforts to ensure that the information provided hereunder is accurate at this date. Avaya may change any underlying processes, architecture, product, description or any other information described or contained in this document. Avaya disclaims any intention or obligation to update or revise the book, whether as a result of new information, future events or otherwise. This document is provided *as is*, and Avaya does not provide any warranty of any kind, expressed or implied.

How this book is organized

In addition to this introduction, *Avaya Aura™ Communication Manager Security Design* contains four major chapters and three appendices. Table 2: Break down of the Communication Manager Security Design guide on page 14 describes each chapter and appendix.

Table 2: Break down of the Communication Manager Security Design guide

Chapter	Description
Introduction	● Communication Manager security philosophy overview on page 15 ● How this guide complements other Avaya product security guides on page 17
Communication Manager Security overview	Describes the security features that Avaya has designed into its products.
Configurable Security	Discusses security issues available within Avaya products that can be enabled for additional security.
	1 of 2

Table 2: Break down of the Communication Manager Security Design guide

Chapter	Description
Network Security Integration	Discusses how to integrate Avaya products securely into an exiting network by leveraging resources, such as Lightweight Directory Access Protocol (LDAP), Active Directory, and Firewalls.
Operational Security	Discusses ongoing activities useful to ensure a high level after the solution has been deployed. Areas include patching, logging, and monitoring.
Appendices	● Appendix C: Physical interfaces and associated network services – Avaya S8300 server on page 247 – Avaya S8400 server on page 249 – Avaya S8500 Series Servers on page 256 – Avaya S8700 Series Servers on page 266 ● Appendix D: Network services on Communication Manager servers ● Appendix E: Additional security resources – Documents mentioned in this security guide on page 287 – Security documents on the Avaya Support site on page 288
	2 of 2

Communication Manager security philosophy overview

This document describes the security-related considerations, features, and services for Communication Manager and its servers. A company's communication system needs to be secure from attacks that cause malfunction or theft of service. Communication Manager inherits a number of mechanisms from legacy communications systems to protect against toll fraud or the unauthorized use of communications resources. However, Communication Manager's IP Telephony capabilities, which converge telephony services with services on the enterprise data network, have the additional need for protections previously specific only to data networking. That is, telephony services need to be protected from security threats such as:

- Denial of Service (DoS) attacks

- Worms
- Viruses
- Theft of data
- Theft of service

Who is responsible for Communication Manager security?

Avaya is responsible for designing and testing its products for security. When Avaya sells a product as a hardware/software package, Avaya's design and testing includes the operating system. In this case, Avaya might also modify the operating system, when necessary for system operation, or when a security vulnerability needs to be resolved.

The customer is responsible for the appropriate security configurations on their data network. The customer is also responsible for using and configuring the security features available on Communication Manager software, on firmware on the Avaya media gateways, and firmware on IP telephones. Avaya, however, offers a service for assessing the customer's network for performance, as well as security, issues. Avaya also offers configuration services for its products.

Responsibility for security updates

When security-related application or operating software updates become available for a Communication Manager system, Avaya tests the updates, if applicable, and then makes them available to customers. In some cases, Avaya modifies the update software and then makes it available to customers.

Avaya notifies customers of the availability of security updates through Security Advisories. Customers can subscribe to be notified about Security Advisories by email. See What is an Avaya Security Advisory on page 163 and How do I get Avaya Security Advisories? on page 164.

When Communication Manager software or media gateway firmware security updates become available, the customer can install the updates or employ an installer from the customer's services support group to install the updates. When an Avaya installer installs the updates, the installer is responsible for following best security practices for server access, file transfers, data backups, and restores. For backups and restores of data, the customer is responsible for providing a secure backup and restore repository on the customer's LAN.

How this guide complements other Avaya product security guides

This document describes security-related issues and security features of Communication Manager, the Communication Manager Servers, and, when applicable, security features of telephones and media gateways. This document is the first in a set of security guides that describe the potential security risks to Avaya products and the features that Avaya products offer to mitigate security risks.

This document is a descriptive guide, *not* a procedural guide. Where appropriate, the guide references other product documentation for the actual procedures for configuring and using security features.

Other product-specific security guides cover the following products:

- Call center products, including Call Management System and Interactive Response
- Integrated Management suite of management tools, including the Avaya Network Console, Secure Access Administration, Fault and Performance Manager, and Avaya Site Administration.
- Unified Communications, including Modular Messaging, Video Telephony Solution, Meeting Exchange, and Web Conferencing, Voice Monitoring Manager, and Provisioning and InstallatIon manager.
- Secure gateways and C360 stackable switches

In addition, the *Avaya Cross-Product Security Guide* describes the high-level security risks and mitigating features offered by the body of Avaya products. This guide seeks to provide background descriptions of IP telephony security risks and to briefly identify security features commonly implemented within Avaya's product line.

Chapter 2: Communication Manager Security overview

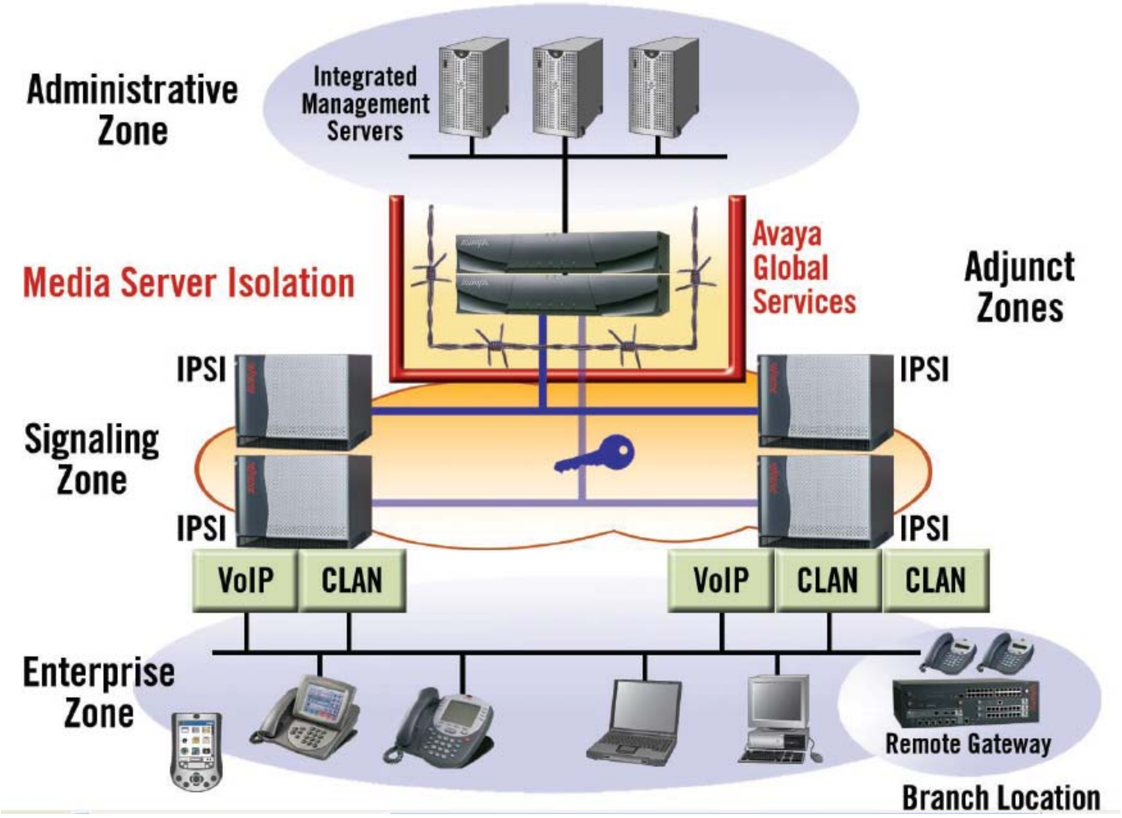
Secure by design

Secure by design encompasses a secure deployment strategy that separates media servers accommodating communication services from the enterprise production network. Media gateways protect and isolate the heart of the Avaya flagship communication solution Communication Manager from viruses, worms, DoS, and malicious attacks.

As can be seen in Figure 1: Avaya secure by design architecture on page 20, the architecture is related to the trusted communication framework infrastructure security layer and allows the design of dedicated security zones for:

- Administration
- Gateway control network
- Enterprise network
- Adjuncts

Figure 1: Avaya secure by design architecture



Avaya isolates assets such that each of the secure zones is not accessible from the enterprise or branch office zones. The zones are like dedicated networks for particular functions or services. They do not need to have access from or to any other zones because they only accommodate the data they are built for. This provides protection against attacks from within the enterprise and branch office zone. The Figure 1: Avaya secure by design architecture on page 20 shows that the only access into the red Media Server zone is from the range of endpoints and branch office gateways intended for signaling traffic.

Gateways with dedicated gatekeeper front-end interfaces (CLAN) inspect the traffic and protect the Media Server zone from flooding attacks, malformed IP packets, and attempts to gain unauthorized administrative access of the Media Server through the Gateways.

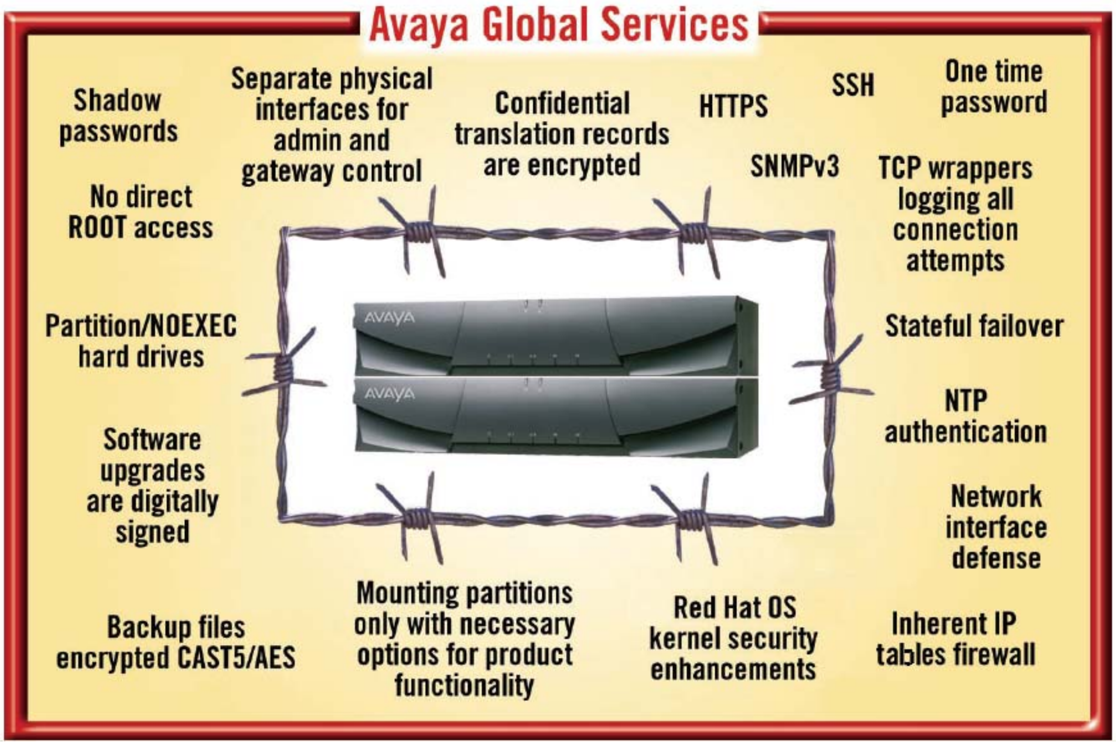
This architecture and framework can also flexibly enhance the virtual enterprise and integrate branch offices into the main corporate network. The security zone from the branch office can terminate at the central Media Gateway interfaces, again protecting the heart of Communication Manager.

Secure by default

Secure by default, the Avaya second security layer, incorporates a hardened Linux operating system with inherent security features for Avaya Media Servers with Communication Manager. This hardened operating system provides only the functions necessary to support the core applications, which is important for securing mission-critical call processing applications and protecting the customer from toll fraud and other malicious attacks. Avaya does not use the standard Linux kernel, but uses a modified kernel. The Avaya kernel is based on the Linux-community offering, but has been changed for secure, real-time telephony processing.

The Linux operating system that Avaya has hardened limits the number of access ports, services and executables. These limits help protect the system from typical modes of attack. At the same time, the reduction of Linux functions reduces the number of mandatory security patches needed and reduces the risk of the narrow *vulnerability-to-exploit* time window.

Figure 2: Avaya Global Services security


Avaya Global Services
Shadow passwords
Separate physical interfaces for admin and gateway control
Confidential translation records are encrypted
HTTPS
SSH
One time password
No direct ROOT access
SNMPv3
TCP wrappers logging all connection attempts
Partition/NOEXEC hard drives
Stateful failover
NTP authentication
Software upgrades are digitally signed
Network interface defense
Backup files encrypted CAST5/AES
Mounting partitions only with necessary options for product functionality
Red Hat OS kernel security enhancements
Inherent IP tables firewall
AVAYA
AVAYA

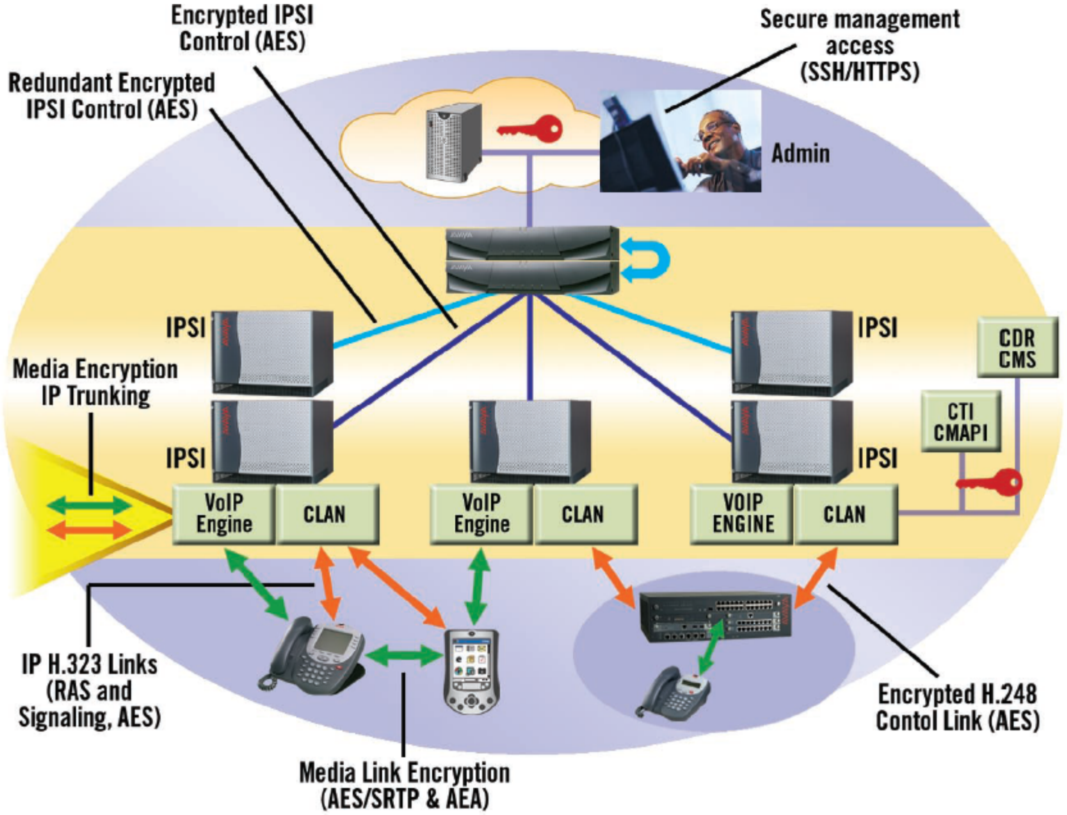
Communication Manager provides a range of in-built functionalities to address the threats posed by malicious software. This functionality minimizes the need for coresident antivirus software, which can interfere with efficient call processing and require continuous administrative attention to ensure antivirus databases are current.

Secure communications

Secure communications, the third layer of Avaya's hardening strategy, uses numerous features and protocols to protect access to and the transmissions from Avaya communications systems. Communication Manager and its media gateways use media encryption to ensure privacy for the voice stream. Alongside media encryption, integrated signalling security protects and authenticates messages to all connected media gateways and IP telephones and eliminates tampering with confidential call information. These features protect sensitive information like caller and called party numbers, user authorization, barrier codes, sensitive credit card numbers and other personal information that is dialed during calls to banks or automated retailers.

Critical adjunct connections, for example the CTI link, which can be separated in a dedicated security zone, can also be encrypted.

Figure 3: Avaya secure communications architecture


Encrypted IPSI Control (AES)
Secure management access (SSH/HTTPS)
Redundant Encrypted IPSI Control (AES)
Admin
IPSI
IPSI
Media Encryption IP Trunking
CDR CMS
CTI CMAPI
IPSI
IPSI
VoIP Engine
CLAN
VoIP Engine
CLAN
VOIP ENGINE
CLAN
IP H.323 Links (RAS and Signaling, AES)
Encrypted H.248 Contol Link (AES)
Media Link Encryption (AES/SRTP & AEA)

Avaya IP endpoints can additionally authenticate to the network infrastructure by supporting supplicant 802.1X. Network infrastructure devices like gateways or data switches act as an authenticator and forward this authentication request to a customer authentication service.

Operating system hardening

Why Avaya chose the Linux operating system for Communication Manager

Avaya uses the open-source Linux operating system as a secure foundation for communications.

Benefits of the open source foundation include:

- Security experts worldwide review the source code looking for defects or vulnerabilities.
- Avaya works diligently to monitor both the enhancements and improvements created by the Linux community and to carefully review the changes before incorporating them into Avaya products.
- Linux-based Avaya servers and gateways protect against many (DoS) attacks such as SYN floods, ping floods, malformed packets, oversized packets, and sequence number spoofing, among others.

Note:

Because of operating system hardening, Communication Manager does not respond to the following:

- ICMP timestamp
- TCP timestamp
- Address-mask queries
- broadcast ping

How Avaya modifies Linux to improve security

Avaya has modified, or hardened, the Linux operating system in several ways to improve minimize vulnerabilities and to improve security.

RPMs removed

The Linux general distribution includes Red Hat Package Management (RPM) modules that install, uninstall, verify, query, and update software packages. Because its IP telephony application needs approximately 30% of the nearly 800 distributed RPMs, Avaya has removed all unused RPMs from the general RPM distribution. For example, two RPMs removed by Avaya are tcpdump unavailability and wireshark (ethereal) packet capturing tools. In addition to making the software file images smaller and more manageable, the operating system is more secure because hackers cannot compromise RPMs that are not present.

To determine which RPMs Avaya employs, use the **`rpm -qa`** command at the Communication Manager server's command line interface (CLI) to see the RPM list.

Unnecessary IP ports closed

Many Linux modules like SSH or Apache or SSL/TLS (HTTPS) are applications that open Ingress network services. Avaya reduces the Ingress network services only to those that are necessary for its telephony applications, thus minimizing exposure of the operating system to network-based attacks. Avaya disables by default less secure network services like TELNET and FTP (see Why using SSH/SCP is more secure than Telnet, FTP, or SNMP on page 26), although customers can enable these services as needed.

Firewall protection

Avaya's Linux-based products use the IPTables firewall that protects against various network-based attacks. The firewall also protects against Ingress services that are enabled through the XINETD mechanism that listens for connection requests or messages on specific ports and starts server programs to perform the services associated with those ports.

The Communication Manager System Management Interface manages the host-based IPTables firewall, allowing customers to control open and closed ports to accommodate their network security requirements.

Drive partitioning

File and directory permissions minimize access as much as possible and act as a preventive measure against malware (see Planning against viruses and worms and other malicious code on page 27) and tampering:

- Executable files are stored in separate hard drive partitions from data.
- Data are stored in separate partitions that do not have execute permissions (the NOEXEC flag).

Linux OS kernel hardening

Avaya compiles Linux with a set of options to precisely tailor its operation to maximize security. Avaya takes the Red Hat Linux distribution and modifies it for the demands of real-time telephony processing, which includes handling finer-grained timing increments. In many cases when the Linux community issues kernel advisories, Avaya is already inherently immune because of its OS kernel modifications.

Privilege escalation and root logins

Avaya's Linux-based products adopt the "privilege escalation" concept that requires lower-privileged accounts to log in at their normal level before they can escalate their privileges to perform more restrictive tasks, such as software replacement. Each privilege escalation requires a password or ASG response and creates a log entry for monitoring.

Tip:
You cannot perform a remote login with root. Only switch users (su) with privilege escalation can achieve a root privilege.

Access Security Gateway

Support accounts (Avaya Services) in installed systems are protected by the Access Security Gateway (ASG), a challenge-response authentication system which replaces passwords for administrative or technical support accounts. Instead of a password, users attempting to login to the server are given a randomly-generated number with which they perform a calculation to determine the correct response. The user is allowed to log in only if they enter the correct response.

ASG supports two encryption types, AES and DES. You must use the AES encryption type for logins created in version 6.0 and later, and the DES encryption type for logins migrated from version 5.2.1 and earlier.

More information

- DoS methods Avaya has designed against on page 28

Why using SSH/SCP is more secure than Telnet, FTP, or SNMP

Connection protocols that send data - especially logins and passwords - in plaintext, that is, unencrypted or "in the clear," can pose a serious security risk to a VoIP enterprise. Using protocols that send data encrypted, such as SSH and SFTP, avoids exposing critical data on the wire. Partly due to new legislation and stricter auditing requirements, Avaya has implemented more secure protocols in its secure connection design.

Disabled by default

By default, Avaya disables these inherently insecure network services:

- TELNET (TELetype NETwork) does not encrypt data (logins, passwords, or PIN information) sent over the connection between the two desired hosts.
- FTP sends information in unencrypted (clear) text, which permits interception by eavesdroppers relatively easily. Also, FTP has no integrity check, meaning that if a file transfer is interrupted, the receiver cannot tell if the transfer is complete.

Note:
If a customer opts to use FTP and/or TELNET, the functionality can be enabled in certain products but is disabled by default.

Avaya products ensure that authentication credentials and file transfers are protected when sent across the network by using:

- Secure Shell (SSH)
- Secure Copy (SCP) or Secure File Transfer Protocol (SFTP)
- SNMP with these stipulations:
  - SNMPv3 is the preferred version due to its built-in security mechanism.
  - SNMPv1 or v2c, while supported, provide only a limited security capability based on community names:
  - The community name for SNMPv1 and SNMPv2c is protected when accessing writable MIBs.

  - For read-only MIBs SNMPv1 and SNMPv2c community names are unprotected.

  SNMP security secrets (for example, community strings) are customer-administrable.

- Other protocols protected using a Transport Layer Security (TLS) or Internet Protocol Security (IPSEC) connection

Avaya Services

Data transmission to and from Avaya Services in support of customer equipment is protected through non-secure data networks like the Internet, over modems, and through SNMP notifications. See *Avaya Enterprise Services Platform Security Overview* (NDA required) for more information.

Planning against viruses and worms and other malicious code

Most viruses and worms (sometimes called "malware") have the effect of

- Disrupting or delaying normal functionality
- Changing configurations by rewriting code
- Retrieving sensitive data

Although similar in their effects, viruses and worms differ in their behavior. A virus needs a host (an application, an e-mail, or a file) and a user action (for example, opening an e-mail attachment) to propagate, but a worm does not need a host or any user action. Viruses and worms are commonly delivered through email, visiting infected Web sites, or sharing file systems. See Table 3: Security impacts from viruses and worms on page 28 for more information.

Table 3: Security impacts from viruses and worms

Security implementation	Security impact
Natural immunity	Avaya's Linux-based servers *do not* support: ● Incoming or forwarding email ● User Web browsing ● Network File System (NFS) or Common Internet File System (CIFS), formerly Server Message Block (SMB), file system sharing protocols
File permissions	Standard program binaries are normally installed with write permissions only to the super-user (root) and cannot be modified, resulting in very few virus outbreaks within the Linux operating system.
Performance degradation	Avaya has tested third-party, host-based antivirus products on its Linux-based servers and uncovered significant performance degradation attributable to the third-party software. Avaya does not recommend installation of such products on its Linux-based servers.
Antivirus products	Customers have successfully used third-party, antivirus packages on select Avaya products even though virus and worm outages have been minimal due to the hardening of the systems. For the customers who prefer to run antivirus software, care should be taken to perform the scan when the server is under little or no load such that impact to the end user is kept to a minimum.

DoS resistance

DoS methods Avaya has designed against

A denial-of-service (DoS) attack occurs when the attacker attempts to make some resource too busy to answer legitimate requests or to deny legitimate users access to the system. Regardless of the method, the net effect of DoS attacks is to shut down a server or an application.

Communication Manager servers survive the DoS attacks listed in Table 4: Avaya's design against types of DoS attacks on page 29 without loss of sanity, without rebooting or restarting, and without reloading, and automatically recover to full service after the DoS attack.

Table 4: Avaya's design against types of DoS attacks

Attack type	Description
SYN flood (TCP SYN)	Phony TCP SYN packets from random IP addresses at a rapid rate fill up the connection queue and deny TCP services to legitimate users.
Land	The Land attack combines IP spoofing with opening a TCP connection. It sends a request to open a TCP connection (SYN flag in the header is on) but changes the IP address so that both the source and destination IP addresses are the same - the destination hose IP address. When the destination host receives the packet, it sets a SYN, ACK to itself because destination and source IP addresses are the same with the same sequence number. The system expects a different sequence number related to the SYN, ACK packet from the other host, so it keeps sending the ACK packet back expecting an updated sequence number. This puts the host into an ACK loop.
Smurf / Pong	Large numbers of ICMP echo (PING) messages sent with the forged address of the intended victim, and Layer 2 devices issue an echo reply (pong), multiplying the traffic by the number of responding hosts.
Fraggle	Like Smurf, Fraggle is a UDP flood that uses an IP broadcast address of the victim (IP spoofing) that results in an infinite loop of echo and reply messages.
Packet replay attack	Packet replay refers to the recording and re-transmission of message packets in the network. Packet replay is a significant threat for programs that require authentication sequences, because an intruder could replay legitimate authentication sequence messages to gain access to a system. An attacker can replay the same packet at different rate, and the system attempts processing duplicate packets causing ● Total resource depletion ● Termination of existing connections ● Chaos and/or confusion in the internal buffers of the running applications ● System crashes in some cases
PING flood	Because so many ping utilities support ICMP echo requests and an attacker does not need much knowledge, sending a huge number of PING requests can overload network links.
	1 of 2

Table 4: Avaya's design against types of DoS attacks

Attack type	Description
Finger of death	The attacker sends finger requests to a specific computer every minute but never disconnects. Failure to terminate the connection can quickly overload the server's process tables. The finger listen port number is 79 (see RFC 742).
Chargen packet storm	The attacker can spoof the chargen service port (19) from one service on one computer to another service on another computer causing an infinite loop and causing loss of performance or total shutdown of the affected network segments.
Malformed or oversized packets	Malformed packets attacks attempt to deny service by causing protocol handlers to cease operation due to the difficulty they have processing odd formations of a protocol or the packets sent as part of the protocol. Oversized attacks place data in an order that is out of specifications or create packets that are larger than the maximum allowed size.
SPANK	The target responds to TCP packets sent from a multicast address causing a DoS flood on the target's network.
SNMP PROTOS	Utilizing the Protos SNMP tool to test SNMP code, an attacker can generate thousands of valid SNMP packets with strange and anomalous values that cause error conditions. (See http://www.ee.oulu.fi)
H.323 / H.225v4PROTOS	As a subset of the widely-deployed H.323 VoIP protocols and standards, H.225v4 deals with the RAS and call signaling, an attacker can generate thousands of valid H.225 packets with strange and anomalous values that cause error conditions. See http://www.ee.oulu.fi
SDP and SIP PROTOS	This attack utilizes the Protos SIP testing tool from OULU University to test SIP code for faulty implementations. The tool generates thousands of valid SIP packets with strange and anomalous values that cause error conditions in the implementation of the protocol. See http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/index.html.
	2 of 2

Additional information

- Recommendations for preventing DoS attacks on page 156

Digital certificates

Security problems addressed by digital certificates

Generally, digital certificates provide:

- Secure authentication — the sender and the recipient validate each other's public key and, therefore, validate each other.
- Data integrity — the data exchanged between the sender and recipient is digitally signed. The recipient can validate the digital certificate and know that the data is not modified.

Communication Manager uses digital certificate when:

- Establishing an HTTPS connection to the Apache Web server for the Communication Manager web interface.
- Establishing SIP-TLS connections.
- The server acts as a repository from which the software or firmware is downloaded to other Avaya devices, primarily H.248 gateways and H.323 endpoints.

Additional information

- How signed firmware provides data integrity assurance on page 31
- Avaya Public Key Infrastructure on page 80
- Secure updates of Avaya software and firmware on page 205

How signed firmware provides data integrity assurance

Digital certificates provide greater security for authentication and data integrity because they:

- Verify that a message really comes from the purported sender by assuming that only the sender knows the private key that corresponds to the public key. Without knowing the private key it is impossible to create a valid digital certificate.
- Timestamp documents. A trusted party signs the document and its timestamp with the private key, thereby assuring that the document existed at the indicated time.

Communication Manager uses digital certificate when transferring software or firmware files between a repository and Communication Manager server or between Communication Manager and other Avaya devices. For example:

- Upgrade firmware and software for Avaya products is signed according to RSA encryption guidelines, and Communication Manager authenticates upgrade file before attempting to install it. If the authentication or certificate does not match, the installation either fails or, in some cases, a warning appears with an option to continue the installation.
- A Communication Manager server provides HTTPS file service for IP telephones. When IP telephones attempt to download firmware from a Communication Manager server over a TLS session, the server provides a certificate for authentication.

Additional information

- Avaya Public Key Infrastructure on page 80
- Secure updates of Avaya software and firmware on page 205

Secure administration

- Access profiles on page 32
- External authentication of server administrator accounts on page 141

Access profiles

Access to Communication Manager, its underlying operating system, and its hardware components (for example, media gateways and IP telephones) is through the System Management Interface and the system access terminal (SAT):

- System Management Interface permit access to system alarms, logs, and diagnostics; permit Communication Manager and media gateway configurations; and security access, configuration, and monitoring.

- The SAT interface permits much the same access and functionality as do the System Management Interface along with different and "deeper" administration, diagnostics, and reports for the Communication Manager application. Examples of "deeper" administration include parameters for stations, trunks, signaling groups, call routing patterns and coverage, and network regions, for which there are no equivalent System Management Interface. Also, there is no access to the Linux operating system through the SAT interface.

Default login accounts that enable access to the System Management Interface and the SAT are similar in that they both use numbered user profiles that generally correspond to Role-Based Access Control (RBAC). They are significantly different in that the interfaces look and operate distinctively, and the account names are not the same.

The profiles and default permissions for these two interface are discussed in:

- System Management Interface default profiles and permissions
- Communication Manager default SAT profiles and permissions

System Management Interface default profiles and permissions

System Management Interface profiles

Table 5: Communication Manager System Management Interface default profiles on page 33 lists and describes the intended use of the default profiles for the System Management Interface.

Note:
Members of the `susers` Linux group have full access to all Web pages. Members of the `users` have access to a limited subset of these pages.

Table 5: Communication Manager System Management Interface default profiles

Profile number	Group	Description
0	suser	Highest level services access; requires secondary user authentication.
1	suser	Designated for service management; requires secondary user authentication.
		1 of 2

Table 5: Communication Manager System Management Interface default profiles

Profile number	Group	Description
2	suser	Designated for Business Partners and must be enabled in the license file. Does not require secondary user authentication.
3	suser	Designated for service technicians; requires secondary user authentication.
4-17		Reserved for future use.
18	suser	Designated for telephony administrators who need the highest access and functionality.
19	user	Permits access to fewer System Management Interface than does Profile 18. Designated for telephony administrators who need lower-level access and functionality.
20-69		Available for customer modification
		2 of 2

System Management Interface default settings

Access permissions to the System Management Interface are administered on the **Security > Web Access Mask** page. Table 6: Communication Manager Web Access Mask default settings on page 35 shows the default access settings for all Communication Manager System Management Interface for Profile 18 and Profile 19. The “X” indicates that the user has access to the corresponding page; a blank denies access to the page.

Avaya recommends using these two profiles as the bases for new user profiles, then adding or restricting permissions to pages in accordance with the customer’s role based access controls (RBAC) or individual security policy.

- **Profile 18** (superuser) permits access to all System Management Interface. Use this profile as the basis for telephony administrators who need the greatest access and functionality. Remove (uncheck) permissions from this profile as necessary when creating new superuser profiles.

- **Profile 19** (user) permits access to fewer System Management Interface than does Profile 18. Use this profile as the basis for telephony administrators who need lower-level access and functionality. Add (check) permissions from this profile as necessary when creating new user profiles.

Table 6: Communication Manager Web Access Mask default settings

Menu-Item	**Fixed (suser)**	**Editable (user)**
	Profile 18	**Profile 19**
Administration		
Licensing	X	X
Native Configuration Manager	X	X
Server (Maintenance)	X	X
Upgrade		
Manage Software	X	
Upgrade Tool	X	
Alarms		
Current Alarms	X	X
Agent Status	X	
SNMP Agents	X	
SNMP Traps	X	
Filters	X	
SNMP Test	X	
Diagnostics		
Restarts	X	X
System Logs	X	X
Temperature/Voltage	X	
Ping	X	
Traceroute	X	
Netstat	X	
Network Time Sync	X	
Raid Status	X	
		1 of 4

Table 6: Communication Manager Web Access Mask default settings

Menu-Item	Fixed (suser)	Editable (user)
	Profile 18	Profile 19
Server		
Status Summary	X	X
Process Status	X	
Interchange Servers	X	
Busy-Out/Release Server	X	
Shutdown Server	X	
Server Date/Time	X	
Software Version	X	X
Server Configuration		
Server Role	X	
Network Configuration	X	
Duplication Parameters	X	
Static Routes	X	
Display Configuration	X	
Eject CD-ROM	X	
Server Upgrades		
Pre Update/Upgrade Step	X	
Make Upgrade Permanent	X	
Boot Partition	X	
Manage Updates	X	
BIOS Upgrade	X	
IPSI Firmware Upgrades		
IPSI Version	X	X
Download IPSI Firmware	X	
		2 of 4

Table 6: Communication Manager Web Access Mask default settings

Menu-Item	**Fixed (suser)**	**Editable (user)**
	Profile 18	**Profile 19**
Download Status	X	
Activate IPSI Upgrade	X	
Activation Status	X	
Data Backup/Restore		
Backup Now	X	X
Backup History	X	X
Schedule Backup	X	
Backup Logs	X	
View/Restore Data	X	
Restore History	X	
Format Local Storage Device	X	
Security		
Administrator Accounts	X	
Login Account Policy	X	
Change Password	X	X
Login Reports	X	
Server Access	X	
Syslog Server	X	
Authentication File	X	X
Firewall	X	
Install Root Certificate	X	X
Trusted Certificates	X	
Server/Application Certificates	X	
		3 of 4

Table 6: Communication Manager Web Access Mask default settings

Menu-Item	Fixed (suser)	Editable (user)
	Profile 18	Profile 19
Certificate Alarms	X	
Certificate Signing Request	X	
SSH Keys	X	
Web Access Mask	X	
Miscellaneous		
File Synchronization	X	
Download Files	X	
CM Phone Message File	X	
Licensing		
License Status	X	X
Feature Administration	X	
		4 of 4

Communication Manager default SAT profiles and permissions

Communication Manager default SAT profiles

Table 7: Communication Manager default SAT profiles on page 39 lists and describes the default profiles for the SAT interface.

Note:
Coresident applications such as CM Messaging or Octel voice mail adjuncts require a standard profile to support TSC access to Communication Manager.

Table 7: Communication Manager default SAT profiles

Profile number	Profile name	Permissions/access	Notes
0	Services superuser	Equivalent to the former SAT *init* login. Has all permissions possible with no restrictions.	Cannot be edited, copied, viewed, or removed. Restricted Requires a second user authentication by Communication Manager.
1	Services manager	Equivalent to the former SAT *inads* login	Cannot be edited, copied, viewed, or removed. Requires a second user authentication by Communication Manager.
2	Business Partner	Equivalent to the former SAT *dadmin* login	Cannot be edited, copied, viewed, or removed. Must be enabled in the license file. The dadmin login can create one login that has craft login permissions and a name other than craft. The second craft login uses Profile 3 and can login without a second challenge.
3	Services	Equivalent to the former SAT *craft* login	Cannot be edited, copied, viewed, or removed. Requires a second user authentication by Communication Manager.
4-15		Reserved for future use by Avaya.	Cannot be edited, copied, viewed, or removed.
16	Call Center manager	Equivalent to the former SAT MIS login (@MIS) CMS/CCR access	Cannot be edited, copied, viewed, or removed. Assign CMS/CCR logins through the MIS application. Note, this is not a "user" login.
17	SNMP	SNMP agent access	Cannot be edited, copied, viewed, or removed.

1 of 2

Table 7: Communication Manager default SAT profiles (continued)

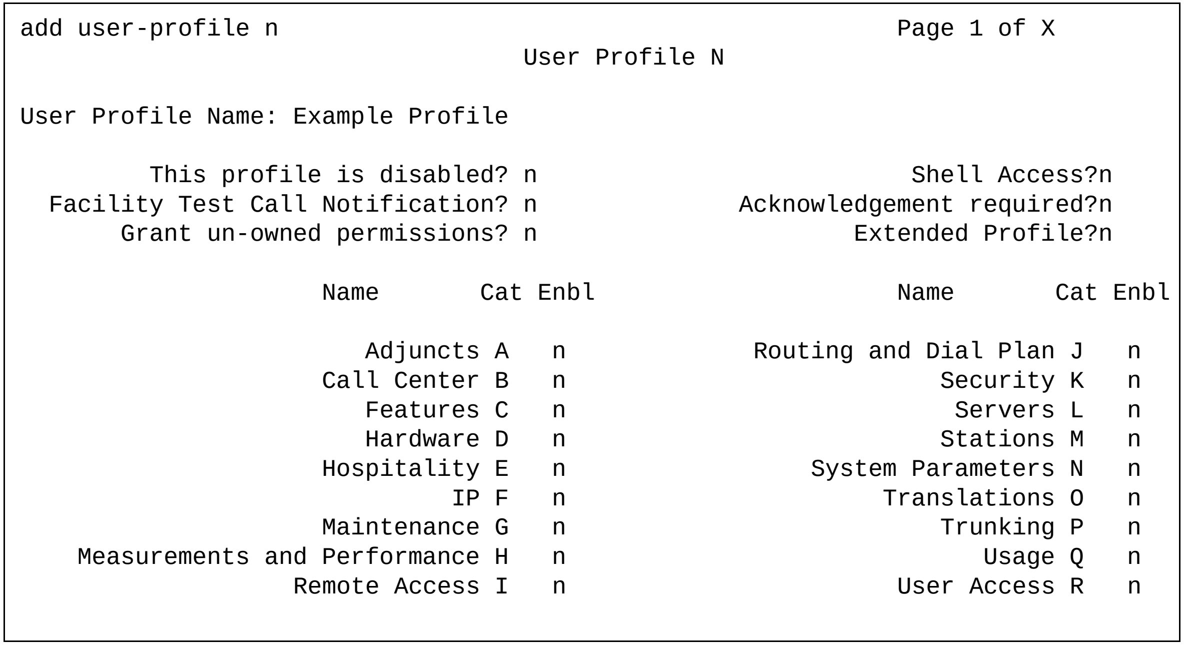
Profile number	Profile name	Permissions/access	Notes
18	Customer superuser	Equivalent to the former SAT default *customer super-user* login	Cannot be edited or removed.
19	Customer user	Equivalent to the former SAT default *non-super-user customer* login	This profile is used during upgrades only. It has no SAT permissions. Cannot be edited or removed.
20-69		Available for customer modification	Use these profile numbers for customized permissions or role-based access control (RBAC).
			2 of 2

Communication Manager profile default settings

The **User Profile** form creates user profiles 20-69 and enables SAT permissions by lettered categories. Each category is associated with a unique set of SAT commands and forms designed to support role-based access control (RBAC) and segmented administration, maintenance, and monitoring.

At the SAT interface, use the **`add user-profile`** ***`n|next`*** to add a new SAT profile and administer its permissions. Use ***`n`*** for the new profile number (20-69) or ***`next`*** for the next number in a sequence. The **Cat** field lists the lettered categories with a brief description in the **Name** field. The default setting is always **n** for the **Enbl** (enable) field for each lettered category, meaning access permissions are not enabled (denied).

Figure 4: Add a new SAT profile



```
add user-profile n                                           Page 1 of X
                                   User Profile N

User Profile Name: Example Profile

         This profile is disabled? n                          Shell Access?n
  Facility Test Call Notification? n             Acknowledgement required?n
       Grant un-owned permissions? n                     Extended Profile?n

                     Name       Cat Enbl                     Name       Cat Enbl

                        Adjuncts A   n             Routing and Dial Plan J   n
                     Call Center B   n                          Security K   n
                        Features C   n                           Servers L   n
                        Hardware D   n                          Stations M   n
                     Hospitality E   n                 System Parameters N   n
                              IP F   n                      Translations O   n
                     Maintenance G   n                          Trunking P   n
    Measurements and Performance H   n                             Usage Q   n
                   Remote Access I   n                       User Access R   n
```

Privilege escalation

Communication Manager supports privilege escalation. Technicians who need higher privileges are required to log in using their normal service accounts and then escalate their privileges to perform more restrictive tasks, for example, software upgrades. An escalation requires a password or ASG response that significantly restricts an intruder from root-level privileges.

To escalate access privileges, a technician uses **sudo**, a Linux/UNIX escalation utility that allows the user to login to another account. The user specifies the account to login to and must correctly respond to the request for the password or one-time-password of that account.

Log entries for privilege escalation and superuser activities appear in different logs:

- Privilege escalation are logged in /var/log/secure.
- Superuser (**su**) operations are logged in /var/log/ecs/commandhistory.

You can read the superuser permissions and restrictions by issuing the **`sudo -l`** command at the server CLI. This command escalates the user’s permissions to the superuser level and the output lists the commands that a superuser can and cannot run on the current host.

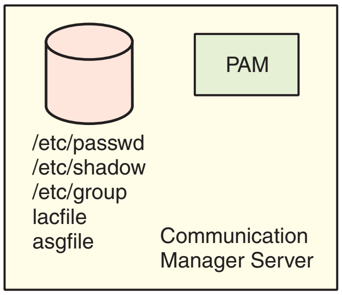
Additional information

- Credentials complexity and expiration requirements on page 99
- Managing administrative accounts on page 110
- Administering authentication passwords on page 111

Local host account authentication

Communication Manager is configured by default to support only local host accounts as shown in Figure 5: Local host accounts on the Communication Manager server. A local host account is an account in which all authentication, authorization, and accounting information is maintained on the same server to which the user is attempting access.

Figure 5: Local host accounts on the Communication Manager server



cycmad01 LAO 032607

- To avoid lockout to the system, you can administer at least one local host account on Communication Manager so that the server is accessible when access to an external AAA server is blocked for any reason. Local host accounts can be used at the same time as any of the external AAA services. The local host configuration on Communication Manager uses the /etc/passwd, /etc/shadow, and /etc/group files, among others.

Chapter 3: Configurable Security

Encryption

- Avaya's encryption overview on page 43
- Transport and storage encryption algorithms on page 44
- Administering encryption in Avaya solutions on page 62
- Mixing encrypted and nonencrypted policies on page 68

Avaya's encryption overview

Digital encryption can reduce the risk of intercepting phone conversations, voice mail, and the signaling messages that support them both. A digital phone call consists of voice (bearer) data and call signaling (control) messages. Both bearer and signaling data can pass through many devices and networks, sometimes over a separate network or virtual path from each other. Without encrypting both data types anyone with access could intercept:

- Digitized voice signals in phone calls and voice mail
- Call signaling messages that:
  - Setup, maintain, and tear down calls
  - Contain call duration
  - Reveal the callers' names and numbers
  - Transmit encryption keys
- Translation (administration) data in transit to or saved on a storage device include IP addresses and routing information from which an attacker can analyze traffic patterns.
- Configuration data through TLS connections

- Application-specific traffic
- Data exchanged during management and administration sessions

Table 8: Comparisons in signaling and bearer traffic on page 44 compares how encryption mitigates the vulnerabilities in signaling and bearer media.

Table 8: Comparisons in signaling and bearer traffic

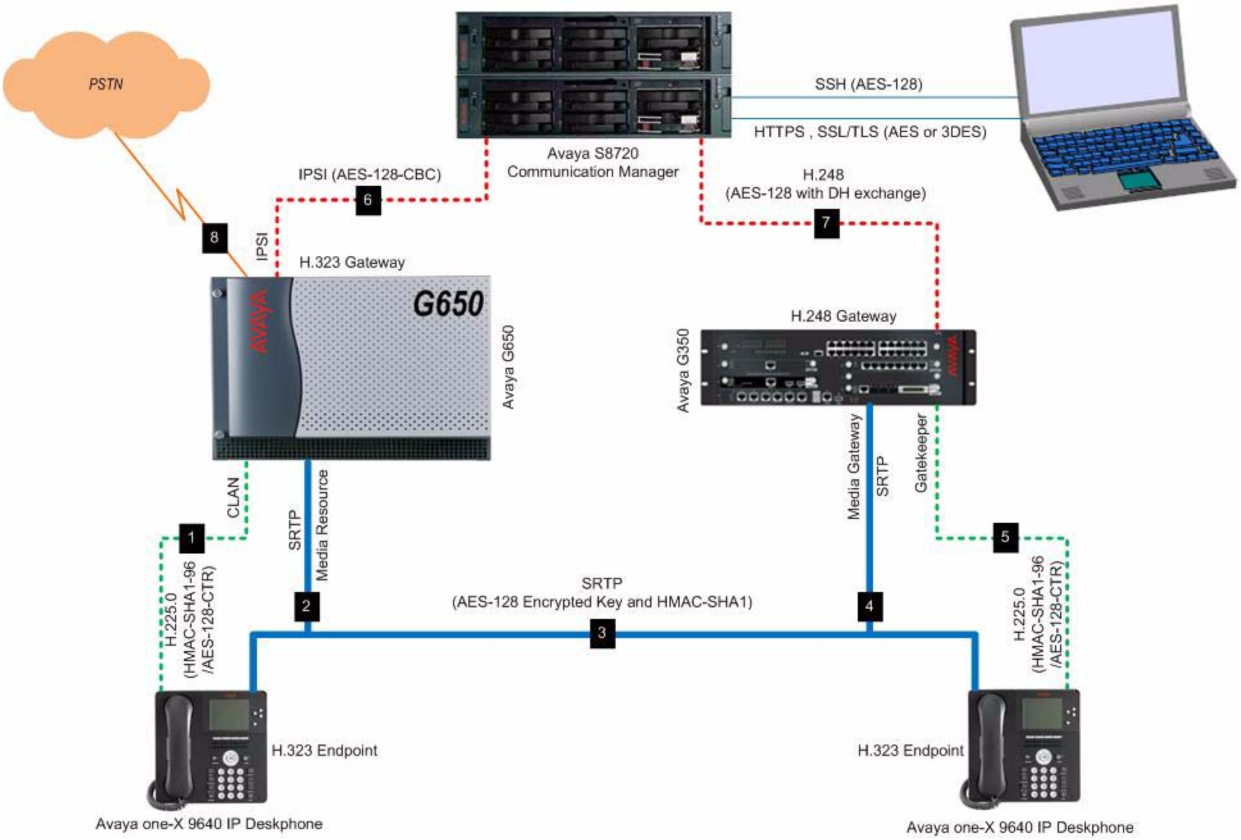
Media	Unencrypted (cleartext)	Encrypted
Bearer	Vulnerable to eavesdropping	Prevents eavesdropping
Signaling	Susceptible to message spoofing and registration hijacking	Prevents message spoofing and hides sensitive information

Transport and storage encryption algorithms

Communication Manager software implements cryptographic algorithms and methodologies that are generally accepted in the INFOSEC community. Furthermore, the selection of cryptographic functions is based on their ability to be approved under a FIPS-140-2 or Common Criteria certification assessment.

Figure 6: Encrypted links in Communication Manager enterprise on page 45 shows the encrypted links in a Communication Manager enterprise.

Figure 6: Encrypted links in Communication Manager enterprise



The following sections describe cryptographic algorithms and key management for the following data links:

- IPSI link security on page 46 (Note 6)
- H.248 link security on page 46 (Note 7)
- H.225.0 Registration, Admission, and Status (RAS) on page 47 and H.225.0 call signaling on page 47 (Notes 1 and 5)
- RTP media encryption on page 48 (Notes 2, 3, and 4)

IPSI link security

The Internet Protocol Server Interface (IPSI) link relays control and signaling information between the IPSI network interface board of the central gateway (for example, G650) and the Communication Manager server. In its signaling function this link is also a conduit between the logical “gatekeeper,” resident in the Communication Manager server, and the H.323 endpoint through the central gateway, see Note 6 for Figure 6: Encrypted links in Communication Manager enterprise on page 45.

The IPSI link is secured using the AES-128-CBC [AES] encryption algorithm to prevent unauthorized access or modification. Inside the encrypted payload, the CRC-16 algorithm is used for error detection and to prevent unauthorized modification of the payload. Since the IPSI link is between only a specific interface card and the Communication Manager server, the key that is used to secure that link needs to be known only by those two entities. AES-128-CBC is dependent on the previous ciphertext block and the current plaintext. Hence, it is unlikely that a cycle of any length can appear unless the transmitted information is identical, which it is not.

H.248 link security

The H.248 link is the data link for control data between the media gateway controller (the Communication Manager server) and H.248 media gateways (Avaya G250, G350, G430, G450, TGM550 and G700 media gateways) through the Gateway Control Protocol. The AES encryption algorithm protects data traversing this link and also includes a simple manipulation detection mechanism (arithmetic sum) inside the encrypted payload. The transport protocol is similar to TLS. The 128-bit symmetric key that protects the data is negotiated between the H.248 gateway and the Communication Manager server using a Diffie-Hellman (DH) key exchange. Each time an H.248 link is established, a new 128-bit symmetric key is negotiated using the DH key exchange.

Once the symmetric key is negotiated, it remains resident in the volatile memory of the media server and gateway, but is not accessible by users or administrators. Since the key is stored in volatile memory, it is destroyed whenever the H.248 link is recreated or whenever the media server or gateway is turned off.

H.225.0 Registration, Admission, and Status (RAS)

Before an H.323 IP endpoint can make a call, it must first register with a gatekeeper. Endpoints register and establish a signaling connection with the gatekeeper (Communication Manager) using the H.323 registration and signaling standard, H.225.0 [ITUH2250]. The first portion of this handshake is the registration (or “RAS”) process between the endpoint and the gatekeeper.

Avaya implements AES encryption and HMAC-SHA-1 authentication algorithms to secure the endpoint registration without exposing any of the authentication credentials of the endpoint (for example, the endpoint’s PIN) to offline attacks. This is achieved while providing registration authentication and replay protection. This authentication process is part of the H.225.0 security profile in H.235.5.

The endpoint and gatekeeper negotiate multiple keys of significant size (128-bits or greater) that are used for authentication of the ongoing registration messages as well as encryption and authentication of the signaling messages. This ensures a secure registration process because it uses the HMAC plus SHA-1 authentication algorithms combined with an encrypted DH key exchange.

Since the keys are negotiated each time the endpoint registers, they are retained only in endpoint and gatekeeper RAM and are not accessible by users or administrators.

H.225.0 call signaling

Once the endpoint has successfully registered, a second H.225.0 signaling link that transmits call-signaling messages is established between the gatekeeper and the endpoint. Examples of these call-signaling messages include button presses, status indicators, and transmission of media encryption keys (when calls are established).

The signaling channel provides both authentication of each packet using the standard HMAC-SHA1-96 algorithm and data encryption. Packets with certain sensitive data elements are transmitted as ciphertext using the AES-128-CTR (counter mode) encryption algorithm. The 128-bit key that is used for encrypting the data is also derived from the master shared secret key that is negotiated during registration.

Similar to H.225.0 RAS, the keys used to authenticate signaling packets and encrypt sensitive elements are dynamically negotiated each time the endpoint registers with the gatekeeper. These keys are stored only in endpoint and gatekeeper RAM and are not accessible by users or administrators. New session keys are created whenever the endpoints are reregister.

RTP media encryption

Avaya supports three high-strength media encryption algorithms, all based on RFC3711:

- Avaya Encryption Algorithm (AEA) a 104-bit, RC4-like encryption algorithm
- Advanced Encryption Standard (AES, 128-bit)
- SRTP

SRTP by default is disabled, you must administratively enable it. For SRTP to work correctly, enable SRTP on the CM trunk side, and administer it using the CM provided administrative tools.

Dynamically-generated, symmetric encryption keys are used for encrypting bearer traffic (voice). Any redirection in the RTP stream generates a new symmetric encryption key sent encrypted from Communication Manager down to H.323 endpoints. In addition to supporting H.235.5 for signaling encryption to the IP phones, Avaya continues to support a challenge/ response authentication method that generates a 56-bit DES encryption key to secure the media encryption keys that are distributed to the H.323 IP endpoints (http://support.avaya.com/elmodocs2/comm_mgr/102882.pdf, p. 4: "H.225.0 Registration, Admission and Status RAS").

SRTP is used with AES 128-bit media encryption key and Avaya supports HMAC-SHA1 80 or HMAC-SHA1 32 for authentication and integrity for each packet, based on the customer’s configuration. H.325 uses the "H.235.8, Key Exchange for SRTP using secure Signaling Channels" for key distribution and H.235.5 to negotiate the 128-bit AES signaling encryption key (http://www.vopsec.net/Avaya_AnnexHPaper110890.pdf) SRTP for SIP uses RFC 4568 "Session Description Protocol (SDP) Security Descriptions for Media Streams" to distribute the media encryption keys. 96xx SIP phones establish a TLS connection to the Avaya SIP Enablement Services (SES) server using 128-bit AES encryption, and SES communicates with Communication Manager using a 128-bit, AES-encrypted TLS connection.

In all of these media encryption solutions, the media encryption keys are dynamically created on a per-connection basis. The keys are created within the gatekeeper and transmitted to the endpoints and media processing boards over the secure links. Additionally, separate keys are produced for the “transmit” and “receive” streams of each call. In the case of conference calls, a unique pair of keys is assigned for encrypting the payload of each endpoint (one for transmit and one for receive). With the introduction of SRTP, derivation of additional keys is performed for authentication of the RTP and RTCP (SRTP) messages.

Since all of these keys are dynamically created and assigned, they are stored only in RAM and are not accessible by administrators or users. RTP keys are not escrowed.

Timers and key exchange details

Key negotiation for IPSI (AES-128-Cipher Block Chaining) and H.248 (AES-128-Output FeedBack) media streams are EKE with 128-bit Diffie-Hellman and fixed symmetric keys. Both are rekeyed whenever a stream is started or reconfigured. The average cycle length for AES/ SRTP with AES-128-CBC is reported to be 2^{127}, which is too long to permit a practical attack. Avaya uses a block size of 128 bits to maximize the average cycle length, for example, with the IPSI link encryption that is dependent on the previous ciphertext block and the current plaintext. Hence, it is unlikely that a cycle of any length can appear unless the transmitted information is identical, which it is not.

SRTP inherently provides anti-replay and integrity protection because once SRTP accepts a packet, it will not accept the same packet again. In addition, packets contain the session key along with the SSRC (synchronization source) that are different for each packet.

Table 9: Encryption supported in Communication Manager

Encryption Technique	Available algorithms	Description
AES		Advanced Encryption Standard (AES), a standard cryptographic algorithm for use by U.S. government organizations to protect sensitive (unclassified) information. Use this option to encrypt these links for: - Server-to-gateway (H.248) - Gateway-to-endpoint (H.323)
AEA		Avaya Encryption Algorithm. Use this option as an alternative to AES encryption when: - All endpoints within a network region using this codec set must be encrypted. - All endpoints communicating between two network regions and administered to use this codec set must be encrypted. Avaya Encryption Algorithm. AEA is not as secure an algorithm as AES but call capacity reduction with AEA is negligible.
SRTP		SRTP provides encryption and authentication of RTP streams for calls between SIP-SIP endpoints, H.323-H.323 endpoints, and SIP-H.323 endpoints. SIP endpoints cannot use AEA or AES encryption.
	1-srtp-aescm128-hmac80	Encrypted/Authenticated RTP with 80-bit authentication tag

1 of 2

Table 9: Encryption supported in Communication Manager

Encryption Technique	Available algorithms	Description
	2-srtp-aescm128-hmac32	Encrypted/Authenticated RTP with 32-bit authentication tag
	3-srtp-aescm128-hmac80-unauth	Encrypted RTP but not authenticated
	4-srtp-aescm128-hmac32-unauth	Encrypted RTP but not authenticated
	5-srtp-aescm128-hmac80-unenc	Authenticated RTP with 80-bit authentication tag but not encrypted
	6-srtp-aescm128-hmac32-unenc	Authenticated RTP with 32-bit authentication tag but not encrypted
	7-srtp-aescm128-hmac80-unenc-unauth	Unencrypted/Unauthenticated RTP
	8-srtp-aescm128-hmac32-unenc-unauth	Unencrypted/Unauthenticated RTP
		2 of 2

Media gateway support

Table 10: Encrypted supported in Avaya media gateways

Model	Version	Supported encryption algorithms
TN2302AP (Medpro)	N/A	Supports AEA or AES ● Extra DSP utilization using AES variant. AES reduces circuit-switched-to-IP call capacity by 25%. **Note:** *Administering Network Connectivity on Avaya Aura™ Communication Manager* http://support.avaya.com.
TN2602AP (IP Media Resource 320)	SRTP support	Supports AEA, or AES, and SRTP ● Does not utilize "extra DSPs" for either method chosen.
TN2312BP (IPSI)		AES-128-Cipher Block Chaining
H.248 Media Gateways (G350, G450, G430, G250)		Supports AEA, or AES (128-Output FeedBack), and SRTP ● Extra DSP Utilization using Avaya Media Encryption AES variant (differs based in Media Gateway) ● Extra DSP utilization using SRTP

Desk phones and client endpoint support

Table 11: Encryption supported in Avaya endpoints

Model	Version	Detail
Avaya IP Softphone Avaya IP Agent	R6 and earlier R7	Supports AEA or AES H.235.5
Avaya one-X Desktop Edition (SIP Softphone)	N/A	Does not support any form of Media Encryption
Avaya one-X Quick Edition	N/A	Does not support Avaya Media Encryption or SRTP
Avaya 3606, 3616, 3620, 3626, 3641, 3645 IP Wireless Phones (VoWLAN)	N/A	Does not support any form of Media Encryption
Avaya 3631 IP Wireless Phone (VoWLAN)	N/A	Supports AES
Avaya IP DECT (3711)	N/A	Does not support any form of Media Encryption
Avaya 46xx (H.323)	See Table 12: Avaya 46XX IP phone firmware versions supporting encryption on page 53.	Supports AEA or AES
Avaya 46xx (SIP firmware)	N/A	Does not support any form of Media Encryption
Avaya 4690 (H.323)	Requires 2.0 firmware or greater	Supports AES
Avaya 96xx (H.323)	1.2 firmware or greater	Supports AES Supports SRTP
Avaya 96xx (SIP firmware) Avaya 9620 Avaya 9630/G Avaya 9640/G	Requires 1.0 firmware or greater Require 2.0 firmware	Supports SRTP
Avaya 16xx one-X Deskphones	N/A	Supports AES

Table 12: Avaya 46XX IP phone firmware versions supporting encryption

46XX phone	Description
Avaya 4606	Not supported
Avaya 4612	Not supported
Avaya 4624	Not supported
Avaya 4630 Avaya 4630SW	Not supported
Avaya 4601	Requires R2.3 firmware or greater
Avaya 4601+ Avaya 4602+ Avaya 4602SW+	Requires R2.3 phone firmware or greater
Avaya 4610SW	Requires R2.3 phone firmware or greater
Avaya 4620 Avaya 4620SW	Requires R2.3 phone firmware or greater
Avaya 4621SW	Requires R2.3 phone firmware or greater
Avaya 4622SW	Requires R2.3 phone firmware or greater
Avaya 4625SW	Requires R2.7 phone firmware or greater

How does media encryption interact with other features?

Media encryption does not affect most Communication Manager features or adjuncts, except for those listed in Table 13: Media encryption interactions with Communication Manager features on page 54.

Table 13: Media encryption interactions with Communication Manager features

Interaction Description	Description
Service Observing	You can Service Observe a conversation between encrypted endpoints. The conversation remains encrypted to all outside parties except the communicants and the observer.
Voice Messaging	Any call from an encryption-enabled endpoint is decrypted before it is sent to a voice messaging system. When the TN2302AP IP Media Processor circuit pack receives the encrypted voice stream, it decrypts the packets before sending them to the voice messaging system, which then stores the packets unencrypted.
Hairpinning	Hairpinning is not supported when one or both media streams are encrypted, and Communication Manager does not request hairpinning on these encrypted connections.
VPN	Media encryption complements virtual private network (VPN) security mechanisms. Encrypted voice packets can pass through VPN tunnels, essentially double-encrypting the conversation for the VPN “leg” of the call path.
H.323 trunks	Media encryption behavior on a call varies based on these conditions at call set up: ● Whether shuffled audio connections are permitted ● Whether the call is an inter-region call ● Whether IP trunk calling is encrypted or not ● Whether the IP endpoint supports encryption ● The media encryption setting for the affected IP codec sets These conditions also affect the codec set that is available for negotiation each time a call is set up. T.38 packets can be carried on an encrypted H.323 trunk, however the T.38 packets are sent in the clear.

Table 14: H.248 gateways encryption interactions with Communication Manager features

Interaction Description	Description
VPN IPSEC	DES-SBC (56-bit) TDES-CBC (168-bit) AES-CBC (128-bit)
SSH2 server	DH (768-2048 bit) TDES-CBC (168 bit) DES-CBC (56-bit) RSA 1024, 2048 DSA 1024, 2048 AES 128 CBC
SNMPv3 agent	DES-CBC (56-bit) HMAC-SHA-1-96 HMAC-MD5-96 AES-CBC (128-bit)
RTP encryption	AES-CBC (128-bit)
Firmware Download Verification	RSA (1024-bit) decryption with SHA-1
License verification	Use RSA (1024-bit) decryption with SHA-1
IP telephony registration	The authentication mechanism is part of H.225 (RAS) registration of IP Voice stations to survivable engine. The authentication uses DES (56-bit) encryption of challenge token with station password PIN as the encryption key.
The TLS client	TDES-CBC, AES-CBC (128, 192, 256 bit).
Secure backup/restore	AES-CBC (128 bit), HMAC-SHA1-32 SRTP: AES-CM (128-bit), HMAC-SHA1-80, HMAC-SHA1-32
ASG-based authentication	Services login authentication, AES-CBC (128-bit)
ASG file encryption	Service login encryption, AES-CBC (128-bit)
AF file download	RSA (1024-bit) with SHA-1 for digital signature verification

Encryption summary

Within Communication Manager, communications are secured from end-to-end using standard encryption and authentication algorithms. Keys are dynamically generated and are stored in RAM where they are overwritten whenever the links disabled or re-created. Additionally, all links support the use of the AES algorithm for encryption using 128-bit keys. When authentication is used, the HMAC-SHA1-96 authentication algorithm is implemented.

Customers can have confidence in Avaya's VoIP solutions because of the implementation of standard encryption and authentication algorithms, use of dynamic key negotiation, and incorporation of this capability as a fundamental part of the standard product offering of Avaya media servers, gateways, and endpoints.

Table 15: Communication Manager secure protocols on page 57 shows that Communication Manager operations are secured from end-to-end using standard encryption and authentication algorithms and key negotiation. Keys are dynamically generated and stored in RAM where they are overwritten whenever the link is disabled or recreated.

Table 15: Communication Manager secure protocols

Link	Description	Transport protocol	Encryption / authentication algorithm	Key exchange
H.248	Server to gateway	Gateway Control Protocol (similar to TLS)	AES-128 with manipulation detection (arithmetic sum)	128-bit symmetric using an encrypted DH exchange. Once negotiated, the key remains in both the server and gateway's volatile memory until the H.248 link is recreated or whenever the server or gateway is turned off. Keys are not accessible by users or administrators.
H.225.0	H.323 IP endpoint to gateway; endpoint authentication credentials not exposed.	RAS	HMAC-SHA1-96 AEAS-128	Encrypted DH exchange: 128-bit encryption and 160-bit authentication, resulting in a 96-bit authentication element for RAS. Keys are negotiated with each registration and are retained in RAM of the IP endpoint and gatekeeper and are not accessible by users or administrators.
				1 of 4

Table 15: Communication Manager secure protocols

Link	Description	Transport protocol	Encryption / authentication algorithm	Key exchange
H.225.0	Signaling between gatekeeper and IP endpoint (for example, button presses, status indicators, and transmission of media encryption keys)	Call signaling	HMAC-SHA1-96 AES-128	All messages sent on the signaling link are encrypted with a DH exchange: 128-bit encryption and 160-bit authentication, resulting in a 96-bit RAS authentication element. Keys are negotiated with each registration and are retained in both endpoint and gatekeeper RAM and are not accessible by users or administrators.
RTP	Bearer traffic (voice calls)	SRTP	AES HMAC-SHA1	Keys are dynamically created on a per-connection basis. Separate keys are produced for the "transmit" and "receive" streams of each call. Keys are not escrowed but are stored in RAM where they are not accessible by administrators or users. In conference calls a unique key pair (one for transmit, one for receive) is assigned for encrypting the payload of each endpoint participating in the conference.
				2 of 4

Table 15: Communication Manager secure protocols

Link	Description	Transport protocol	Encryption / authentication algorithm	Key exchange
Administrative access	SAT interface for server to computer/ laptop	SSH	AES-128	SSH client on administrator's PC negotiates with the server to determine which cipher suite is used. Keys negotiated each time link is established and are discarded at the end of the session (not retained in flash memory).
	Web interface for server to computer/ laptop	HTTPS SSL/TLS	AES 3DES	Keys negotiated each time link is established and are discarded at the end of the session (not retained in flash memory).
IPSI	Control and signaling information between Internet Protocol Server Interface (IPSI) in a central gateway to the server		AES-128-CBC	Pre-administered key stored in IPSI flash memory and CM software but not accessible by users or administrators exchanged with 128-bit Diffie-Hellman. Since the IPSI link is only between a specific interface card and the media server, the key that is used to secure that link only needs to be known by those two entities.

3 of 4

Table 15: Communication Manager secure protocols

Link	Description	Transport protocol	Encryption / authentication algorithm	Key exchange
Account information	Required local account stored on media server; all others on supported external AAA server.			
Backup	Server to data destination: files in the pam_config backup set are included in the security set. For manual movement to another server running the same Communication Manager release.	SCP	AES-128	15-256 character pass phrase
				4 of 4

Additional information

- [AES] Advanced Encryption Standard, FIPS-197, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
- [DH] W. Diffie and M.E. Hellman, “New Directions in Cryptography,” IEEE Transactions in Information Theory, v. IT-22, n. 6, Nov 1976, p. 664-654
- [EKE] Bellovin and Merritt, U.S. Patent 5,241,599, August 31, 1993, assigned to Lucent Technologies, AT&T Bell Laboratories.
- [GNUPG] www.gnupg.org
- [HMAC] H. Krawczyk, M. Bellare, and R. Canetti, HMAC: Keyed-Hashing for Message Authentication,

- IETF Informational RFC 2104, February 1997.
- [HTTPS] E. Rescorla; “HTTP over TLS”; RFC 2818, http://www.ietf.org/rfc/rfc2818.txt
- [ITUH2250] ITU-T Recommendation H.225.0, "Call signaling protocols and media stream packetization for packet-based multimedia communication systems."
- [ITUH235H] ITU-T H.235 Amendment 1, "Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals," Annex H.
- [RHSG] The Official Red Hat Security Guide, http://www.redhat.com/docs/manuals/linux/RHL-8.0-Manual/pdf/rhl-sg-en-80.pdf
- [SHA1] FIPS PUB 180-1, Secure Hash Standard, U.S. Department of Commerce, Technology Division, National Institute of Standards and Technology, April 17, 1995.
- [SRTP] Baugher, Carrara, Naslund, Norman; “SRTP: The Secure Real Time Transport Protocol,” IETF.
- RFC Pending, http://www.ietf.org/internet-drafts/draft-ietf-avt-srtp-09.txt
- [SSHWG] IETF Secure Shell Working Group (secsh), multiple IETF Internet Drafts, http://www.ietf.org/html.charters/secsh-charter.html
- [TLS] T. Dierks, C. Allen; “The TLS Protocol,” IETF 2246, http://www.ietf.org/rfc/rfc2246.txt

Administering encryption in Avaya solutions

Administering encryption in Communication Manager CODEC sets, Network Regions, and signaling groups is done through the System Access Terminal (SAT) interface:

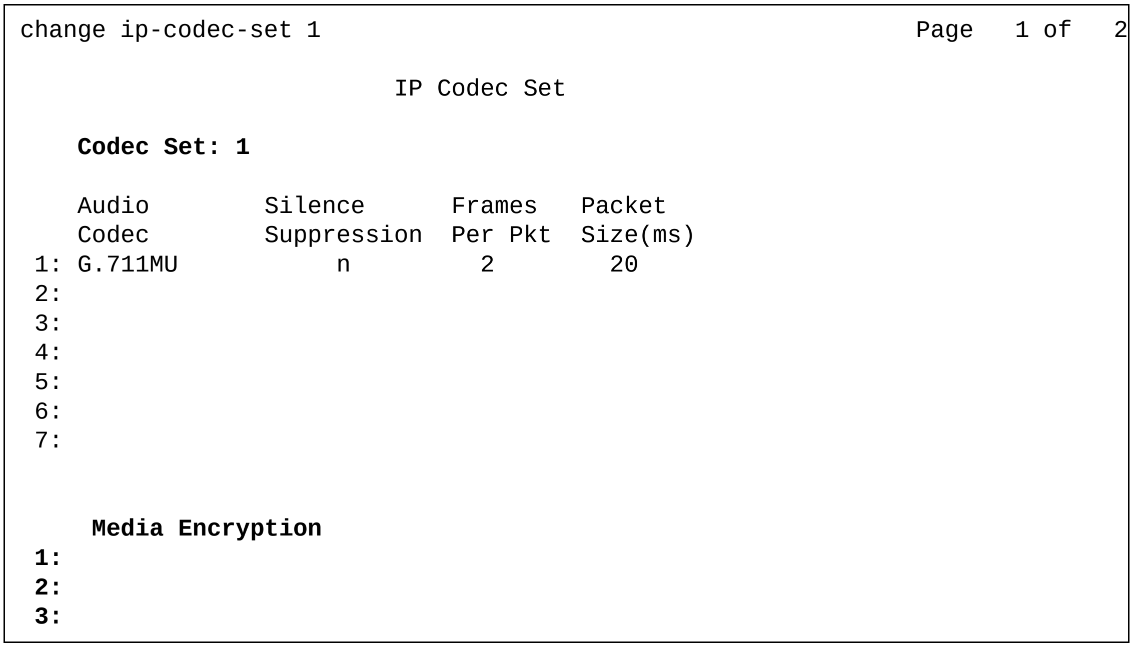
- SAT administration for IP CODEC Sets and Network Regions discusses how Communication Manager assigns an encryption algorithm to each supported CODEC (COder-DECoder) and applies the CODEC's encryption policy to similarly-provisioned IP endpoints through its Network Regions. Network Regions are established either through SAT administration for IP CODEC Sets and Network Regions or through the Network Region Wizard (NRW).
- SAT administration for signaling groups discusses how Communication Manager can encrypt IP signaling groups.

SAT administration for IP CODEC Sets and Network Regions

The first step to Communication Manager encryption administration involves assigning an encryption algorithm to a CODEC on the **IP Codec Set** form. Administer the Network Regions form by issuing the **`change ip-network-region`** ***n*** command from the System Access Terminal (SAT).

Tip:

If you are unfamiliar with which CODEC sets are available in Communication Manager, type **`list ip-codec-set`** at the SAT to display a list or press **Help** while the cursor is on any of the numbered list of CODECs.



```
change ip-codec-set 1                                         Page   1 of   2

                          IP Codec Set

    Codec Set: 1

    Audio         Silence      Frames   Packet
    Codec         Suppression  Per Pkt  Size(ms)
 1: G.711MU            n          2        20
 2:
 3:
 4:
 5:
 6:
 7:


     Media Encryption
 1:
 2:
 3:
```

The available encryption algorithms are listed and described in Table 16: Communication Manager administrable encryption algorithms on page 64.

⚠ **Important:**

SRTP encryption is supported by 96xx telephones only.

The **Media Encryption** field on the **IP Codec Set** form appears only when the **Media Encryption** field is set to **y** on the Customer Options form and the **Media Encryption over IP** feature is enabled in the license file.

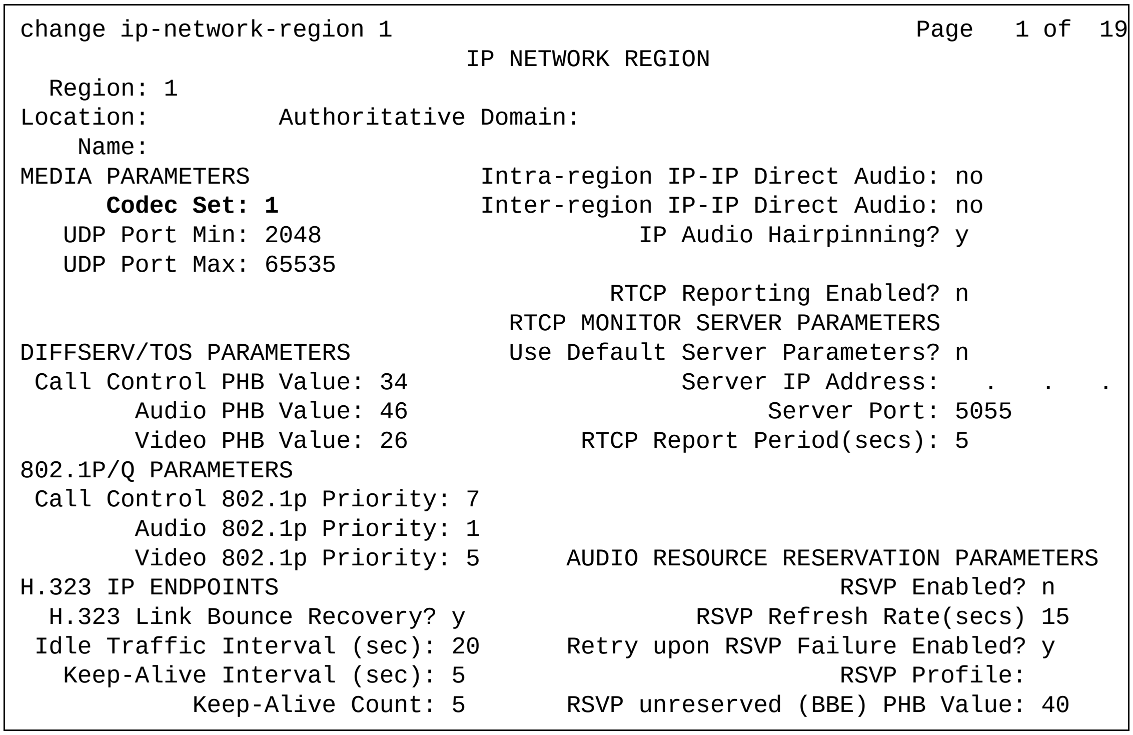
Table 16: Communication Manager administrable encryption algorithms

Valid Media Encryption entries	Usage
aes	Advanced Encryption Standard (AES), a standard cryptographic algorithm for use by U.S. government organizations to protect sensitive (unclassified) information. Use this option to encrypt these links: ● Server-to-gateway (H.248) ● Gateway-to-endpoint (H.323)
aea	Avaya Encryption Algorithm. Use this option as an alternative to AES encryption when: ● All endpoints within a network region using this codec set must be encrypted. ● All endpoints communicating between two network regions and administered to use this codec set must be encrypted.
1-srtp-aescm128-hmac32	Encrypted/Authenticated RTP with 32-bit authentication tag
2-srtp-aescm128-hmac80 **Note:** The only supported SRTP value for stations is **srtp-aescm128-hmac80**. H.323 IP trunks support all eight of the listed SRTP algorithms.	Encrypted/Authenticated RTP with 80-bit authentication tag
3-srtp-aescm128-hmac32-unauth	Encrypted RTP but not authenticated
4-srtp-aescm128-hmac80-unauth	Encrypted RTP but not authenticated
5-srtp-aescm128-hmac32-unenc	Authenticated RTP with 32-bit authentication tag but not encrypted
	1 of 2

Table 16: Communication Manager administrable encryption algorithms

Valid Media Encryption entries	Usage
6-srtp-aescm128-hmac80-unenc	Authenticated RTP with 80-bit authentication tag but not encrypted
7-srtp-aescm128-hmac32-unenc-unauth	Unencrypted/Unauthenticated RTP
8-srtp-aescm128-hmac80-unenc-unauth	Unencrypted/Unauthenticated RTP
none	Media stream is unencrypted (default)
	2 of 2

The second part of administering Communication Manager encryption involves assigning codecs) to network regions. Administer the **IP Network Region** form by issuing the **change** **`ip-network-region`** ***n*** command from the System Access Terminal (SAT).



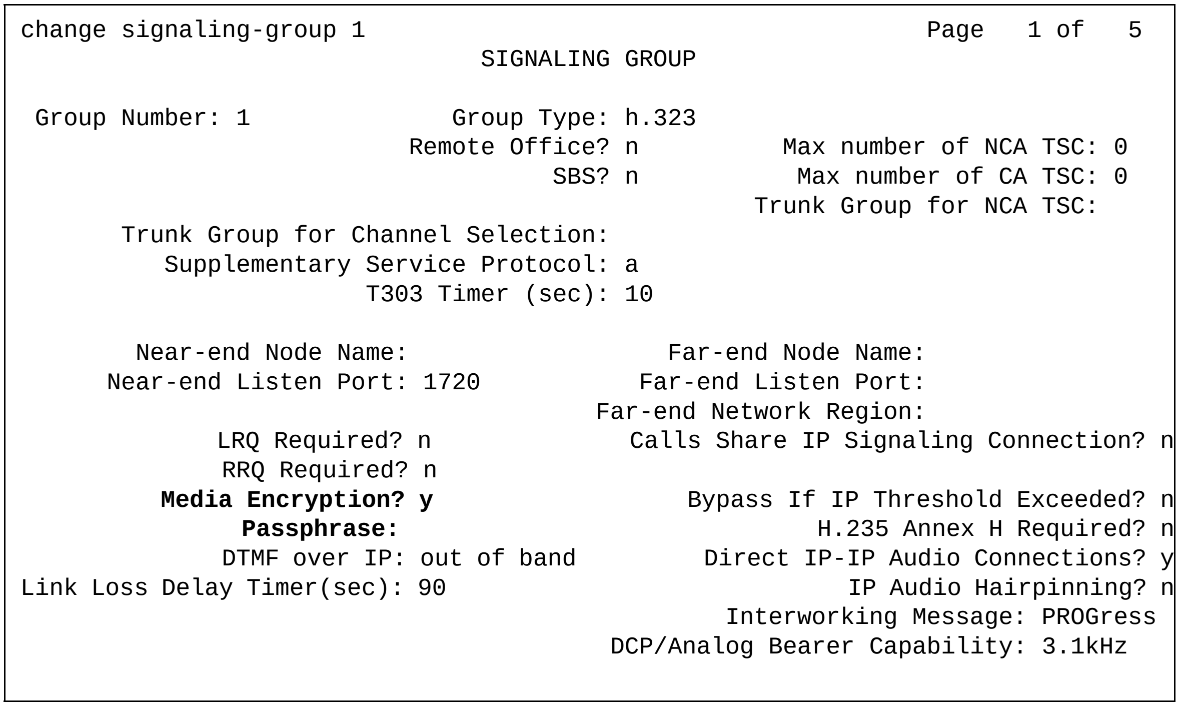
```
change ip-network-region 1                                    Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain:
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: no
      Codec Set: 1              Inter-region IP-IP Direct Audio: no
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   UDP Port Max: 65535
                                         RTCP Reporting Enabled? n
                                  RTCP MONITOR SERVER PARAMETERS
DIFFSERV/TOS PARAMETERS           Use Default Server Parameters? n
 Call Control PHB Value: 34                   Server IP Address:   .   .   .
        Audio PHB Value: 46                         Server Port: 5055
        Video PHB Value: 26                RTCP Report Period(secs): 5
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 7
        Audio 802.1p Priority: 1
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y                RSVP Refresh Rate(secs) 15
 Idle Traffic Interval (sec): 20      Retry upon RSVP Failure Enabled? y
   Keep-Alive Interval (sec): 5                          RSVP Profile:
            Keep-Alive Count: 5       RSVP unreserved (BBE) PHB Value: 40
```

The **IP Network Region** form requires that you specify a CODEC set, having already administered the encryption algorithm earlier. Network Regions allow you to apply an encryption scheme to all of the IP endpoints within the region.

By contrast, see Mixing encrypted and nonencrypted policies on page 68 for more information about applying heterogeneous encryption policies across more than one Network Region.

SAT administration for signaling groups

Communication Manager encryption administration for signaling groups involves enabling encryption on the **Signaling Group** form. Administer this form by issuing the **change `signaling-group`** ***n*** command from the System Access Terminal (SAT).



```
change signaling-group 1                                       Page   1 of   5
                                SIGNALING GROUP

 Group Number: 1              Group Type: h.323
                           Remote Office? n          Max number of NCA TSC: 0
                                     SBS? n           Max number of CA TSC: 0
                                                   Trunk Group for NCA TSC:
       Trunk Group for Channel Selection:
          Supplementary Service Protocol: a
                        T303 Timer (sec): 10

        Near-end Node Name:                  Far-end Node Name:
      Near-end Listen Port: 1720           Far-end Listen Port:
                                        Far-end Network Region:
              LRQ Required? n             Calls Share IP Signaling Connection? n
              RRQ Required? n
          Media Encryption? y                 Bypass If IP Threshold Exceeded? n
                Passphrase:                            H.235 Annex H Required? n
              DTMF over IP: out of band        Direct IP-IP Audio Connections? y
Link Loss Delay Timer(sec): 90                           IP Audio Hairpinning? n
                                                 Interworking Message: PROGress
                                         DCP/Analog Bearer Capability: 3.1kHz
```

Important:

The **Media Encryption** field on the **Signaling Group** form appears only when the **Media Encryption** field is set to **y** on the Customer Options form and the **Media Encryption over IP** feature is enabled in the license file.

- A **y** in the **Media Encryption?** field enables encryption on trunk calls using this signaling group.

- The **Passphrase** field requires an 8- to 30-character string.

> ⚠ **Important:**
> See “Administering Media Encryption for signaling groups” in *Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)* for a complete discussion of signaling group encryption and caveats regarding end-to-end trunk and passphrase administration.

Network Region Wizard

The Avaya Network Region Wizard (NRW) is a browser-based wizard that is available on Communication Manager servers. The NRW guides you through the steps required to define network regions and set all necessary parameters though a simplified, task-oriented interface. For a system that has several network regions, the NRW saves time for system provisioners as well as helps configure the system for optimum IP performance.

Additional information

- Mixing encrypted and nonencrypted policies on page 68.

- “Administering IP network regions” and “Administering Media Encryption for signaling groups” in *Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)*.

- For more information about using Network Regions, see this application note http://www.avaya.com/master-usa/en-us/resource/assets/applicationnotes/advantages_of_implem.pdf.

- For more information on configuring Network Regions in Communication Manager, see this application note http://www.avaya.com/master-usa/en-us/resource/assets/applicationnotes/netw-region-tutorial.pdf.

- The NRW Job Aid and worksheet are available at http://support.avaya.com/avayaiw.
- "Configuring Avaya Communication Manager for Media Encryption," a white-paper, is available at http://www.avaya.com/master-usa/en-us/resource/assets/applicationnotes/media-encrypt.pdf.

Mixing encrypted and nonencrypted policies

Administering encryption in Avaya solutions on page 62 focuses on groups of *similar* IP endpoints and common network resources. This section contains information about administering network regions for *different* IP endpoint groups based upon location or network characteristics. Creating separate network regions, each with its own encryption scheme, then interconnecting the regions can apply encrypted and nonencrypted policies across the enterprise.

“Administering inter-network region connections” in *Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)* contains information about administering network regions, including topics related to interconnecting regions with disparate provisioning, specifically:

- Inter-Network Region Connection Management
- Call Admission Control and bandwidth consumption
- Inter-Gateway Alternate Routing (IGAR) mapping between network regions
- Port network-to-network region mapping for non-IP boards
- Status/monitoring commands for inter-region bandwidth usage

Additional information

- Administering encryption in Avaya solutions on page 62

- “Administering inter-network region connections” in *Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)*
- Call Admission Control and bandwidth consumption in *Avaya Application Solutions: IP Telephony Deployment Guide (555-245-600)*

Authentication files for Communication Manager

The authentication file contains Access Security Gateway (ASG) keys and the server certificate for Communication Manager. ASG keys make it possible for Avaya Services to securely access the customer’s system.

System Platform and Communication Manager share the same authentication file. A default authentication file is installed with System Platform. However the default file must be replaced with a unique file. Unique authentication files are created by the Authentication File System (AFS), an online application at http://rfa.avaya.com. After you create and download the authentication file, you install it from the System Platform Web Console of the Communication Manager server. When you install the authentication file in System Platform, the file is automatically installed on Communication Manager, Utility Server, and any other virtual machines on the server.

Every time that you upgrade Communication Manager to a new major release, you need to create and install a new authentication file.

⚠ **Important:**
Installing the authentication files also installs the Avaya digital certificate for Communication Manager.

Authentication files for duplicated servers and survivable servers

For duplicated pair configurations, you must install the same authentication file on both the active server and standby server. The authentication file is not synchronized from the active server to the standby server.

Each survivable server must have its own unique authentication file. A unique file must be installed from the System Platform Web Console of each server.

About the authentication file

AFS authentication files have a plain text XML header with encrypted authentication data and an encrypted server certificate.

Each authentication file contains an authentication file ID (AFID) that identifies it. You need this AFID to create a new authentication file for an upgrade or to replace the current authentication file on the server.

ASG

ASG is a challenge-response mechanism that replaces the use of passwords with a mechanism that challenges the user differently for each login. When a user attempts to log in to an ASG-enabled account on the server, the system displays a randomly generated number instead of a request for a password. The user must use a tool such as ASG Web Mobile to obtain the appropriate response to the challenge. The user is allowed to log in only if he or she enters the correct response.

Starting the AFS application

Prerequisites

AFS is available only to Avaya and Avaya Partners. If you are a customer and need an authentication file, contact Avaya or your authorized Avaya Partner.

You must have a login ID and password to start the AFS application. You can sign up for a login at http://rfa.avaya.com.

1. Type http://rfa.avaya.com in your Web browser.

2. Enter your login information and click **Submit**.

3. Click **Start the AFS Application**.

   A security message is displayed.

4. Click **I agree**.
   The AFS application starts.

Creating an authentication file for a new system

You can choose to download the authentication file directly from the AFS application to your computer, or you can have the authentication file sent in an e-mail message.

1. Start and log in to the AFS application.
2. In the **Product** field, select **SP System Platform**.
3. In the **Release** field, select the release number of the software, and then click **Next**.
4. Select **New System**, and then click **Next**.
5. Enter the fully qualified domain name (FQDN) of the host system where Communication Manager is installed. For duplicated Communication Manager servers, enter the alias FQDN.
6. Enter the FQDN of the Utility Server.
7. If you want to download the authentication file directly from the AFS application to your computer:
    1. Click **Download file to my PC**.
    2. Click **Save** in the File Download dialog box.
    3. Select the location where you want to save the authentication file, and then click **Save**.
    4. Click **Close** in the Download complete dialog box to complete the download.

       After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).
8. If you want to have the authentication file sent in an e-mail message:
    1. Enter the e-mail address in the **Email Address** field.

b. Click **Download file via email**. AFS sends the e-mail message that includes the authentication file as an attachment and the AFID, system type, and release in the message text.

c. Save the authentication file to a location on the e-mail recipient's computer.

   After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).

9. To view the header information in the authentication file, go to the location where the file is saved and use WordPad to open the file.

   The header includes the AFID, product name and release number, and the date and time that the authentication file was generated.

Related topics:

Starting the AFS application on page 70

Creating an authentication file for a file replacement

Prerequisites

You must have the AFID of the authentication file that you want to replace. See Obtaining the AFID from System Platform Web console on page 76 or Obtaining the AFID from Communication Manager SMI on page 76.

You can choose to download the authentication file directly from the AFS application to your computer, or you can have the authentication file sent in an e-mail message.

1. Start and log in to the AFS application.
2. In the **Product** field, select **SP System Platform.**
3. In the **Release** field, select the release number of the software, and then click **Next**.

4. Select **Upgrade or Re-deliver for Existing System**.

5. In the **Authentication File ID** field, enter the AFID for the authentication file that is currently installed on the system, and then click **Next**.

6. Select one of the following options:

   - If you use an Avaya Services login to access Communication Manager, read the product access instructions. After reading the instructions, select **I read and understand the Product Access Instructions**.

   - If you do not use an Avaya Services login to access Communication Manager, select **I do not use Avaya Services logins**.

7. If you want to download the authentication file directly from the AFS application to your computer:

   a. Click **Download file to my PC**.

   b. Click **Save** in the File Download dialog box.

   c. Select the location where you want to save the authentication file, and then click **Save**.

   d. Click **Close** in the Download complete dialog box to complete the download.

   After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).

8. If you want to have the authentication file sent in an e-mail message:

   a. Enter the e-mail address in the **Email Address** field.

   b. Click **Download file via email**. AFS sends the e-mail message that includes the authentication file as an attachment and the AFID, system type, and release in the message text.

c. Save the authentication file to a location on the e-mail recipient's computer.

After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).

9. To view the header information in the authentication file, go to the location where the file is saved and use WordPad to open the file.

   The header includes the AFID, product name and release number, and the date and time that the authentication file was generated.

Related topics:

Starting the AFS application on page 70

Obtaining the AFID from System Platform Web console on page 76

Obtaining the AFID from Communication Manager SMI on page 76

Creating an authentication file for an upgrade to a new major release

Prerequisites

You must have the AFID of the authentication file on the system that you are upgrading. See Obtaining the AFID from System Platform Web console on page 76 or Obtaining the AFID from Communication Manager SMI on page 76.

You can choose to download the authentication file directly from the AFS application to your computer, or you can have the authentication file sent in an e-mail message.

1. Start and log in to the AFS application.

2. In the **Product** field, select **SP System Platform**.

3. In the **Release** field, select the release of software to which you are upgrading, and then click **Next**.

4. Select **Upgrade or Re-deliver for Existing System**.

5. In the **Authentication File ID** field, enter the AFID for the authentication file that is currently installed on the system, and then click **Next**.

6. Select one of the following options:

    - If you use an Avaya Services login to access Communication Manager, read the product access instructions. After reading the instructions, select **I read and understand the Product Access Instructions**.

    - If you do not use an Avaya Services login to access Communication Manager, select **I do not use Avaya Services logins**.

7. If you want to download the authentication file directly from the AFS application to your computer:

    a. Click **Download file to my PC**.

    b. Click **Save** in the File Download dialog box.

    c. Select the location where you want to save the authentication file, and then click **Save**.

    d. Click **Close** in the Download complete dialog box to complete the download.

    After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).

8. If you want to have the authentication file sent in an e-mail message:

    a. Enter the e-mail address in the **Email Address** field.

    b. Click **Download file via email**. AFS sends the e-mail message that includes the authentication file as an attachment and the AFID, system type, and release in the message text.

c. Save the authentication file to a location on the e-mail recipient's computer.

After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).

9. To view the header information in the authentication file, go to the location where the file is saved and use WordPad to open the file.

   The header includes the AFID, product name and release number, and the date and time that the authentication file was generated.

Related topics:

Starting the AFS application on page 70

Obtaining the AFID from System Platform Web console on page 76

Obtaining the AFID from Communication Manager SMI on page 76

Obtaining the AFID from System Platform Web console

1. Start and log in to the System Platform Web Console.

2. In the navigation pane, click **User Administration > Authentication File.** The AFID is displayed in the **AFID** field. An AFID of 7100000000 is the default authentication that is installed with System Platform. The default file must be replaced with a unique file.

Obtaining the AFID from Communication Manager SMI

1. Start and log in to the Communication Manager System Management Interface (SMI).

2. Click **Administration > Server (Maintenance)**.

3. In the navigation pane, under **Security**, click **Authentication File**. The AFID is displayed in the **AFID** field. An AFID of 7100000000 is the default authentication that is installed with System Platform. The default file must be replaced with a unique file.

Installing an authentication file

Prerequisites

You must create and download the authentication file from AFS.

System Platform and Communication Manager share the same authentication file. When you install the authentication file in System Platform, the file is automatically installed on Communication Manager, Utility Server, and any other virtual machines on the server. However, the suser account must be created on Communication Manager for the authentication file to be installed on Communication Manager.

Once the suser account is created, the authentication that is installed on System Platform (default or unique), is automatically installed on Communication Manager. The authentication file must be installed on Communication Manager for you to log in to Communication Manager.

1. Start and log in to the System Platform Web Console.
2. Click User **Administration > Authentication File**.
3. Click **Upload.**
4. In the Choose File to Upload dialog box, find and select the authentication file, and then click **Open**.

Note:
To override validation of the AFID and date and time, select **Force load of new file** on the Authentication File page. Select this option if you:

- need to install an authentication file that has a different unique AFID than the file that is currently installed, or

- have already installed a new authentication file but need to reinstall the original file

  You do not need to select this option if you are replacing the default authentication file with a unique authentication file.

⚠ **CAUTION:**
Use caution when selecting the **Force load of new file** option. If you install the wrong authentication file, certificate errors and login issues may occur.

5. Click **Install**.
   The system uploads the selected authentication file and validates the file. The system installs the authentication file if it is valid.

6. To confirm that the authentication file is installed on Communication Manager, check the Authentication File page of the SMI.

Related topics:

Obtaining the AFID from Communication Manager SMI on page 76

Digital certificates and server trust relationships

- Chain of trust on page 78
- Avaya Public Key Infrastructure on page 80
- PKI in Communication Manager on page 83
- Managing changes to the Avaya certificate on page 96

Chain of trust

Digital certificates certify that a public key belongs to its reputed owner. To ensure greater trust, a trusted party can sign the public key and the information about its owner, creating a public-key certificate, usually called a certificate. Similar to a driver’s license, a certificate guarantees the identity of its bearer.

A trusted party that issues digital certificates is called a certification authority (CA), similar to a governmental agency that issues drivers' licenses. A CA can be an external certification service provider or even a government, or the CA can belong to the same organization as the entities it serves. CAs can also issue certificates to other sub-CAs, which creates a tree-like certification hierarchy called a public-key infrastructure (PKI).

Communication Manager servers require that their unique certificate chain of trust reverts back to the root CA. The chain of trust consists of the:

- Server certificate, signed by a Remote Feature Activation (RFA) Issuing Authority (IA)
- RFA IA certificate, signed by the Avaya Product Root Certificate Authority (CA)
- Root certificate for the Avaya Product CA

The server certificate and the IA certificate are embedded in the authentication file along with the private key associated with the certificate. The Avaya Product Root CA certificate is embedded in the Communication Manager software base, not in the authentication file.

Avaya RFA uses a:

- FIPS 140-2 level 4 certified cryptographic module to sign media server certificates.
- Certificate daemon to:
  - Generate public/private key pairs using OpenSSL
  - Obtain digital certificates for media server certificates
  - Retrieve a copy of the IA certificate

The secure hardware and daemon ensure that media server certificates are stored securely, are used only for the purpose of signing authorized certificates, and are protected from unauthorized access or duplication.

Avaya Public Key Infrastructure

Public Key Infrastructure (PKI) combines software, encryption technologies, and services to enable enterprises to secure their communications and transactions over data networks. A successful PKI provides the management infrastructure for integrating public key technology (digital certificates, public keys, and certificate authorities) across the customer’s infrastructure, including IP telephony.

The goal is to conduct electronic business with the confidence that:

- The sending process/person is actually the originator.
- The receiving process/person is the intended recipient.
- Data integrity is not compromised.

Avaya uses standard X.509 PKI to manage certificates in the enterprise in which the hierarchy of certificates is always a top-down tree, with a root certificate at the top, representing the central Certificate Authority (CA) that is integral to the trusted-party scheme and does not need third-party authentication. From Communication Manager 6.0 Avaya certificates are installed with the installation of the authentication files. Prior to Communication Manager 6.0 there were only self-signed digital certificates.

The Avaya product PKI is limited to device-to-device authentication primarily to automatically establish a TLS or similar connection to ensure confidentiality, integrity, and authenticity. VoIP devices that use Avaya software or need to establish a TLS connection with other devices that are manufactured or distributed by Avaya (or used in coordination with Avaya products) use certificates issued by CAs or downloads from Signing Authorities (SAs) under the Avaya Product PKI.

Communication Manager uses a consistent PKI model, including the:

- Private key located in `/etc/opt/ecs/certs/cm/private/server.key`
- Certificate located in `/etc/opt/ecs/certs/cm/ID/server.crt`
- Trusted CA certificates located in `/etc/opt/ecs/certs/cm/CA/all-ca.crt`

Table 17: Key pair and certificate usage on page 81 lists the Avaya public and private keys and their uses.

Table 17: Key pair and certificate usage

Entity	Key type	Uses
Subscriber	Private key	● Digital certificates ● Encryption In some cases the subscriber private key is used specifically for signing code.
Relying party	Public key	● Authenticate digitally-signed software and firmware downloads ● Authenticate TLS connections

Note:
The Avaya Product Certificate Authority does *not*:

- Publish subscriber certificates, but it does archive copies of certificates
- Notify other entities of certificates that it has issued
- Issue certificates to individuals

Avaya security certificate types

The Avaya server uses two types of security certificates, a Root or a Certificate Authority (CA) certificate and a server certificate.

A Root or CA certificate establishes Avaya Inc. as a trusted CA. You must install a root certificate after you log in. This certificate allows your browser to trust the server certificate that the Avaya server presents after configuration.

A server certificate verifies the identity of a server. The server certificate changes every time the server is reconfigured. If the server's name is changed the next time you log in you may get a security alert.

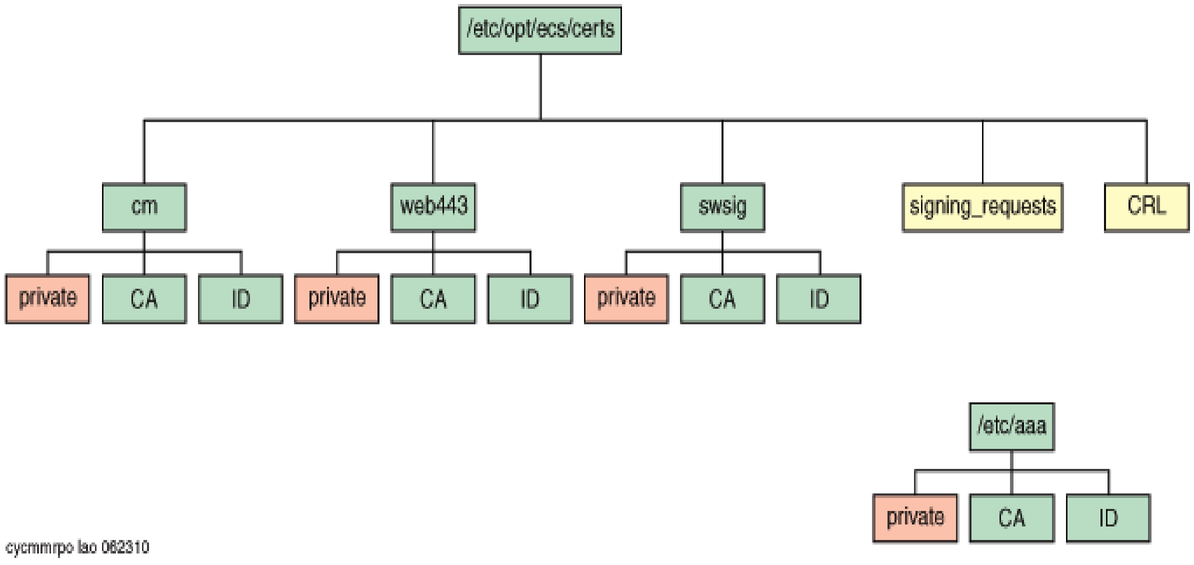
The Avaya server relies on two server certificates. One server certificate is the default certificate used by service technicians (who must log in to many servers to perform tasks). The default certificate is issued to the services Ethernet interface address (`192.11.13.6`) and identifies the certificate authority as the *SIP Product Certificate Authority.*

The second server certificate is issued to a site-specific Avaya server (such as, SIP-TLS and HTTPS). After this server certificate is configured, its name is unique to that particular site's server.

⚠ **Important:**
Before you can log into the Avaya server you must accept or store the server certificate.

Avaya certificate repository

Digital certificates in Communication Manager are stored in a few fixed directories. These directories are known as certificate repositories.



PKI in Communication Manager

Communication Manager uses digital certificates for authentication during TLS session establishment, per the TLS standard to:

- Establish SIP/TLS connections between IP phones and Communication Manager through the customer-installed, trusted third-party certificate (Customers can install their own trusted certificates on page 90).
- Establish connections between IP phones and Communication Manager through Avaya's trusted chain (PKI in H.323 and SIP endpoints on page 92) for the purpose of securing configuration downloads and firmware updates to the IP phone.
- Download configuration data from Communication Manager for file synchronization (Filesync to duplicated or survivable servers on page 96).
- Authenticate access to the Communication Manager Web interface (Connection to Communication Manager Web interface on page 96)
- SIP/TLS connections
  - Management
  - Signaling

Install Root Certificate on a PC

The Install Root Certificate page allows you to install the security certificate that contains the Avaya digital signature. The security certificate with the Avaya digitial signature prevents unauthorized users from intercepting and viewing passwords and other sensitive information.

The Root Certificate establishes Avaya Inc. as a trusted Certificate Authority (CA). You must install the Root Certificate after you log in.

⚠ **WARNING:**
You must install a CA certificate as a Root Certificate.

If you do not install the Root Certificate you will get a Security Alert stating that the company is not trusted.

Installing a Root Certificate on a PC

1. From the **Avaya Aura Communication Manager (CM) System Management Interface (SMI)** page select **Install Root Certificate**.
2. From the **Install Root Certificate** page click **Install**.
3. In the **File Download - Security Warning** dialog box click **Save**.
4. Select a location and save the *avayaRootCert.cer*.
5. Navigate to the location for *avayaRootCert.cer* and double-click it.
6. In the **Open File - Security Warning** dialog box, click **Open**.
7. From the **General** tab in the **Certificate** dialog box, click Install **Certificate...**.
8. Accept all the default settings in the **Certificate Import Wizard**, and click **Finish**.

⚠ **Important:**

The root certificate name is user-defined. In this guide the root certificate name *avayaRootCert.cer* is used only as an example.

Trusted certificates

The **Trusted Certificates** page allows you to manage the trusted certificate repositories for the server. All the installed certificates are listed on the **Trusted Certificates** page. Use this page to install a certificate, copy an existing certificate to other repositories, or remove a certificate from repositories.

⚠ **Important:**
A trusted certificate must be a Certificate Authority (CA) certificate.

Displaying a trusted certificate on the server

- From the **Trusted Certificate** page, select a certificate entry, and click **Display**.

Adding a trusted certificate to the server

⚠ **Important:**
A trusted certificate must be a Certificate Authority (CA) certificate.

1. From the **Trusted Certificates** page, click **Add**.

2. From the **Trusted Certificate - Add** page enter the file name for the certificate you want to add. The certificate must be in a pem file *and* in the `/var/home/ftp/pub` directory.

3. To validate the certificate, click **Open**.
   After a successful validation, the **Trusted Certificates – Add** page displays the issued-to, issued by, and expiration date information for the certificate you are adding.

Note:
An error message is displayed if the certificate is not a valid certificate.

4. Enter a name for the certificate. Give the certificate, you are adding, the same name in each repository.

5. Select the repositories you want the certificate added to, and click **Add**.
   The system verifies the following:

   a. The certificate name has a `.crt` extension. If the certificate name has a different extension, the system deletes it and replaces it with a `.crt` extension.

   b. The certificate name is unique and does not already exist.

   c. The certificate is not a duplicate certificate with a new name.

Deleting a trusted certificate from the server

1. From the **Trusted Certificate** page, select a certificate entry, and click **Remove**.

2. From the **Trusted Certificate - Remove** page select the repositories you want the certificate deleted from, and click **Remove**.

Removing a trusted certificate on the server from a particular repository

See Deleting a trusted certificate from the server on page 86.

Copying a trusted certificate on the server from one repository to another repository

1. From the **Trusted Certificate** page, select a certificate entry, and click **Copy**.

2. From the **Trusted Certificates – Copy** page select the repositories where you want the certificate copied to, and click **Copy**.
   The system verifies the following:

   a. The certificate name is unique and does not already exist.

   b. The certificate is not a duplicate certificate with a new name.

Note:
If the certificate fails to install in one repository, it does not mean that the certificate failed to get installed in the other selected repositories.

Server and application certificates

A server certificate verifies the identity of a server. A server certificate changes every time the server is reconfigured. It binds the certificate name to a public key and this is used to verify the identity of a server.

⚠ **Important:**
You must update the server certificate every time you change the server name.

The Avaya server provides two server certificates. One certificate is for the service technicians who must log in to many servers. The service technicians' certificate is issued to the services Ethernet interface address (`192.11.13.6`), and identifies the certificate authority as the Avaya Call Server. The second certificate is issued to the site-specific server name after it is configured.

You must accept or store the server certificate before you can log in to the Avaya server. Insure that you have a secure connection to the server.

The **Server/Application Certificates** page allows you to manage both server and application certificate repositories for the server. The **Server/Application Certificates** page displays all the installed certificates, and allows you to install, remove and copy an existing certificate to another repository.

Note:
The server certificate must be signed by at least one of the CAs in the chain of trust. That is, one of the CAs in that certificate must be part of the Communication Manager trusted certificates repository.

Displaying a server or application certificate

1. From the **Server/Application Certificates** page, select a certificate and click **Display**.
2. Click **Back** from the **Server/Application Certificates - Display** page to return to the main **Server/Application Certificates** page.

Adding a server or application certificate to the server

⚠ **WARNING:**
You must be a member of the susers group to add a server or application certificate.

Prerequisite:

Communication Manager must include at least one corresponding Certificate Signing Request (CSR), or a private key must be appended to the server certificate.

1. From the **Server/Application Certificates** page, click **Add**.
2. From the **Server/Application Certificates - Add** page, enter the file name of a certificate in `/var/home/ftp/pub` that contains the certificate chain you want to add. The certificate must be either a PKCS#12 file or a file in pem format.
3. Enter the password of the certificate you are adding (if required).
4. To validate the certificate click **Open**.
   After a successful certificate verification, the following information is displayed on the **Server/Application Certificates - Add** page:
   - issued to
   - issued by
   - date of expiration

5. Select the appropriate repositories (where the certificates are to be installed) and click **Add**.

Note:
To store the certificate the system will not prompt you to enter a file name. The default file name is `server.crt`.
In the case of a single server and application certificate chain, the server sub-directory of a repository is limited to a single file for a single certificate chain. This file is the server.crt file. This certificate represents an identity, and only one identity is supported. The system overwrites the existing `server.crt` file, and replaces it with the new one.

Removing a server or application certificate from the server

⚠ **WARNING:**
You must be a member of the susers group to add a server or application certificate.

1. From the **Server/Application Certificates** page, select a certificate and click **Remove**.
2. From the **Server/Application Certificates - Remove** page select the certificate to remove from a single repository, or if the certificate is installed in more than one repository, from an arbitrary combination of repositories.
3. Click **Remove**.

Copying a server or application certificate to different repository on the same server

⚠ **WARNING:**
You must be a member of the susers group to add a server or application certificate.

1. From the **Server/Application Certificates** page, select a certificate and click **Copy**.
2. From the **Server/Application Certificates - Copy** page, select the repository you want install the selected certificate to. You can choose more than one repository.
3. Click **Copy**.

Customers can install their own trusted certificates

Communication Manager and other applications running on a Communication Manager server rely on trusted certificates for secure interoperation.

Every time it starts, Communication Manager loads the following trusted certificates in its repository into its runtime memory:

– Avaya Product Root Certificate Authority
– SIP Certificate Authority
– Motorola SSECA Root Certificate Authority
– Spectel Root Certificate Authority

All of these certificates are concatenated in the **all-ca.crt** file in the repository.

By using the `tlscertmanage` command (see Additional information on page 99) at the server command line, customers can load a third-party trusted certificate into the Communication Manager repository for use the next time Communication Manager restarts.

Note:
You must restart Communication Manager before it can recognize and use the newly-installed third-party certificate.

The **all-ca.crt** file can contain up to eight (8) certificates, meaning that the customer may load up to four additional third-party certificates. If more than 8 certificates are in the **all-ca.crt** file, Communication Manager loads the first eight then ignores the remaining certificates and generates a minor alarm (see Additional information on page 99) and a syslog entry to notify the user that it could not load the file.

Third-party certificate management

Table 18: Communication Manager third-party certificate management on page 91 describes how Communication Manager handles third-party certificates.

Table 18: Communication Manager third-party certificate management

Activity	Description
File sync	To prevent overwriting a customer-installed, third-party certificate, file sync does not synchronize any certificates.
Upgrades	1. Copy the third-party certificate file to the server. 2. Execute the `tlscertmanage` command to add the certificate to the trusted repository. 3. After the upgrade, re-install the third-party certificate with the `tlscertmanage` command. **Note:** Avaya does not recommend deleting the original certificate file. However, if the original file was deleted, then you must copy it to the server again.
Backup / restore	Backup and restore software does not back up or restore trusted certificates.

PKI in H.323 and SIP endpoints

The Avaya Product Certificate is embedded in IP endpoint firmware and serves these purposes:

- Before downloading firmware upgrades to IP phones, Communication Manager validates the embedded certificate before downloading the firmware file to the IP phone. The embedded certificate cannot be viewed from any standard interface, including the phone.
- Authenticates the SIP Enablement Services (SES) server (Avaya One-X 96XX SIP phone only).

Note:
Avaya IP (H.323) phones do not verify whether the Communication Manager identity certificate has expired but do verify the chain of trust for the incoming Communication Manager certificate.

IP phones are typically provisioned in a staging area where the certificate authority and a Web server are on a physically-separated LAN. The IP phones download the certificate parameters from the Web server and perform a certificate request using the Simple Certificate Enrollment Protocol (SCEP) protocol. Once the certificates are provisioned in the IP phones, they can be moved and used anywhere in the enterprise.

The digital certificate, private key, and trusted-CA certificates are stored in flash in the IP phone. The same certificate can also be used for 802.1x authentication and for SIP/TLS authentication.

When the IP phone boots, it reads the 46xxsettings.txt file that contains these certificate-related parameters:

- URL for the Certificate Authority
- List of trusted certificates to download to the phone
- Certificate Common Name (CN)
  - $SERIALNO for the phone’s serial number
  - $MACADDR for the phone’s MAC address

Note:
The CN in the phone certificate is typically the phone’s serial number, however the CN is not used in SIP signaling.

- Certificate Distinguished Name
- Certificate Authority Identifier
- Certificate Key Length

- Certificate Renewal Threshold
- Certificate Wait Behavior

Table 19: Certificate usage in Avaya endpoints on page 93 lists the certificate usage in Avaya H.323 phones (96XX, 46XX, and 16XX) and SIP phones (Avaya One-X 96XX).

Table 19: Certificate usage in Avaya endpoints

Phone type	Certificate	Use/Description
96XX (H.323)	Avaya Product Root Certificate Authority Trust Certificates **Note:** Beginning with 46XX H.323 Release 2.9 firmware and 96XX H.323 Release 2.0 firmware customers can import trusted third-party certificates to the phone using the TRUSTCERT parameter.	Download configuration files port trusted certificates **Note:** Includes 46xxsettings.txt, 46xxupgrade.scr, 96xxupgrade.txt, etc. downloaded through the Communication Manager HTTPS server.
46XX (H.323)	Avaya Product Root Certificate Authority Trust Certificates **Note:** Beginning with 46XX H.323 Release 2.9 firmware and 96XX H.323 Release 2.0 firmware customers can import trusted third-party certificates to the phone using the TRUSTCERT parameter.	Download configuration files Import trusted certificates **Note:** Includes 46xxsettings.txt, 46xxupgrade.scr, 96xxupgrade.txt, etc. downloaded through the Communication Manager HTTPS server.
		1 of 3

Table 19: Certificate usage in Avaya endpoints

Phone type	Certificate	Use/Description
16XX (H.323)	Avaya Product Root Certificate Authority	Download configuration files **Note:** Includes 46xxsettings.txt, 46xxupgrade.scr, 96xxupgrade.txt, etc. downloaded through the Communication Manager HTTPS server.
		2 of 3

Table 19: Certificate usage in Avaya endpoints

Phone type	Certificate	Use/Description
96XX SIP	Avaya Product Root Certificate Authority **Note:** Simple Object Access Protocol (SOAP) between the 96XX SIP phones and SES by default uses HTTP but can be configured for HTTPS, in which case the Avaya Product Root Certificate Authority (CA) certificate authenticates the SES server through the signed CA identity certificate. x.509 Identity Certificate **Tip:** Customers can replace the default identify certificate using the Simple Certificate Enrollment Protocol (SCEP, see Additional information on page 99).	Download configuration files over HTTPS, when enabled. Establishes a SIP/TLS connection to the Avaya SIP Enablement Services (SES) server and utilized if 802.1X EAP/TLS is enabled. **Note:** Uses TLSSRVR, TSLPORT, HTTPSRVR, and HTTPPORT parameters in the DHCP Option #242. The TLS connection from the SIP phone to the SIP Enablement Services (SES) server is encrypted using TLS_RSA_WITH_AES_128_CBC_SHA.
SIP Softphone	Hard-coded certificate	SIP Softphone firmware includes a default phone certificate. **Note:** However, Avaya recommends using a uniquely-provisioned phone certificate installed through Simple Certificate Enrollment Protocol (SCEP, see Additional information on page 99).
		3 of 3

Connection to Communication Manager Web interface

Communication Manager ships with a non-unique default certificate that establishes an HTTPS connection to the Apache Web server for the Communication Manager Web interface. The certificate is accepted when the license installation is complete, and the server is fully operational. The server certificate is stored in `/etc/opt/ecs/certs/web443/ID` and requires root access to view.

Filesync to duplicated or survivable servers

Duplicated Avaya S8700 Series Servers use filesync to send the server certificates from the active server to the standby, as the certificates are required in the standby server in case it is called into service. Filesync creates a TCP SSL/TSL socket between the active and standby servers, establishing an encrypted link to transfer the contents of the /etc/opt/ecs/certs directory. using the TLSv1 protocol for the transmission.

Communication Manager also uses filesync to download configuration data to an Enterprise Survivable Server (ESS) for file synchronization.

Managing changes to the Avaya certificate

Table 20: Changes in the Avaya certificate on page 96 lists how Avaya manages changes to its digital certificates.

Table 20: Changes in the Avaya certificate

Type of change	Description
Renewal	Certificates are never renewed. In the event that a certificate expires or is compromised, a new certificate is issued along with a new license file.
Re-key	Certificates are never re-keyed. In the event that a certificate expires or is compromised, a new certificate is issued along with a new license file.
	1 of 2

Table 20: Changes in the Avaya certificate

Type of change	Description
Modification	Certificates are never modified. In the event that certificate content needs to change, a new certificate is issued along with a new license file.
Revocation	Certificates are revoked if the customer, technical support, or members of the Avaya Security Team believes the certificate has been compromised for any reason. Final decision is left to the Avaya Product Certificate Authority. A certificate is revoked in these circumstances: ● The information in the certificate is wrong or inaccurate. ● The subject has failed to comply with the rules in the policy. ● The system to which the certificate has been issued has been retired or is no longer supported.
Who can request revocation?	Certificate revocations can be requested by: ● The certificate subscriber ● The Registration Authority (RA) that has performed the validation of the certificate request ● Any entity presenting proof of responsibility for a certified Avaya SIP product ● Any entity presenting proof of the certificate misuse ● Any entity presenting proof of the private key compromise The final decision on revocation of the certificate is left to the Avaya Product Certificate Authority.
Procedure for revocation request	The Avaya Product Certificate Authority accepts revocation requests by email only: apca@avaya.com The email must be authenticated and must include the serial number and subject name of the certificate in question.
Revocation request grace period	Avaya determines a timeframe for response at the time of the request.
	2 of 2

Certificate alarms

The system administrator can generate an early notification alarms for impending expiration of certificates.

Major alarms are automatically generated seven days before the certificate expires and also on the day the certificate expires on the server.

You cannot disable or reconfigure these two alarms. You can only remove or replace the expired certificate.

Creating certificate alarms

The **Certificate Alarms** page allows you to configure alarms at three different time periods before the first automatically generated alarm. The first automatically generated alarm occurs seven days before the certificate expiration date.

1. From the **Avaya Aura Communication Manager (CM) System Management Interface (SMI)** page select **Certificate Alarms**.

2. From the **Certificate Alarms** page select one or all of the following options:

   - Create an warning alarm or a minor alarm between 61 - 180 days before the certificate expires.
   - Create an warning alarm, a major alarm, or a minor alarm between 31 - 60 days before the certificate expires.
   - Create a major alarm or a minor alarm between 8 - 30 days before the certificate expires.

3. For each option you selected above choose the type of warning you want to set from the drop-down box, and the day you want the alarm generated.

4. Click **Submit**.

Additional information

- Remote Feature Activation (RFA) Web site: http://rfa.avaya.com

- Replacing the identify certificate using Simple Certificate Enrollment Protocol (SCEP) in *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Installation and Maintenance Guide* (http://support.avaya.com/elmodocs2/9600/16_601943_2.pdf)

- Information about the `tlscertmanage` command is in *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers (03-300431)*.

- Information about the alarm generated by incorrect third-party certificate administration is in *Maintenance Alarms for Avaya Aura™ Communication Manager, Media Gateways and Servers (03-300430)*.

Administrative accounts

- Credentials complexity and expiration requirements on page 99
- Credentials management on page 103
- Applying profiles for role-based administration on page 104
- Managing administrative accounts on page 110
- Administering authentication passwords on page 111

Credentials complexity and expiration requirements

Communication Manager logins comply with:

- Password complexity policies on page 100

- Credentials expiration and lockout policies on page 101

Password complexity policies

Password complexity rules that apply to passwords for local administrator and user accounts are listed in Table 21: Password complexity rules for Communication Manager. Attempts to create disallowed passwords result in an instructive error message.

Table 21: Password complexity rules for Communication Manager

Password complexity rules	Parameters
Minimum length	Default is 6.
Number of previous passwords that must not match	Default is 1.
No repeated and/or sequential characters	Communication Manager enforces the rules.
Check passwords against common dictionary words, vendor names, and other words to add to a “no use” list.	Communication Manager performs the audit.

Table 22: Password complexity rules for Branch Gateways

Password complexity rules	Parameters
Minimum length	8 characters.
Number of previous passwords that must not match	No memory of previous passwords.
Check passwords against common dictionary words, vendor names, and other words to add to a “no use” list.	RADIUS server with gateways perform the validation.

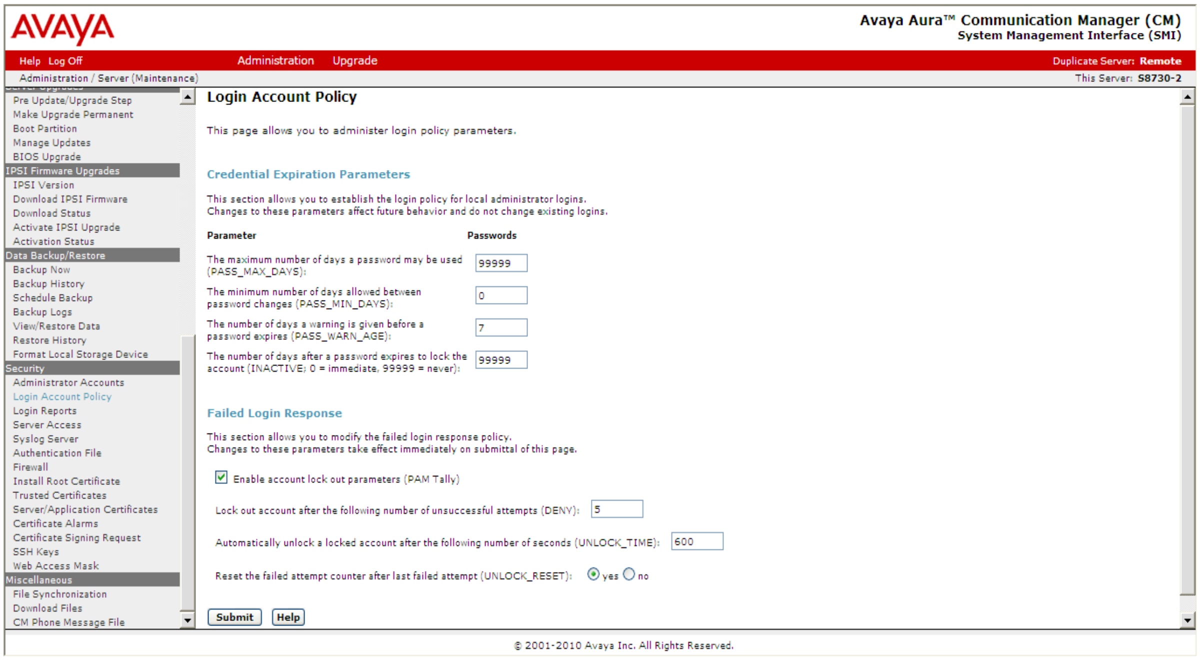
Credentials expiration and lockout policies

To apply expiration and lockout policies for administrator logins, go to **System Management Interface > Security > Login Account Policy**.

Note:
This page sets global policy for all logins created through the Server (Maintenance). Logins whose credentials are maintained on an external AAA server or logins that by design are outside the global policy must be administered with the “root” login using standard Linux commands.

Note:
Credentials expiration and lockout policies for branch gateways are managed through gateways CLI.

Figure 7: Login Account Policy page



Login Account Policy

This page allows you to administer login policy parameters.

Credential Expiration Parameters

This section allows you to establish the login policy for local administrator logins.
Changes to these parameters affect future behavior and do not change existing logins.

Parameter	Passwords
The maximum number of days a password may be used (PASS_MAX_DAYS):	99999
The minimum number of days allowed between password changes (PASS_MIN_DAYS):	0
The number of days a warning is given before a password expires (PASS_WARN_AGE):	7
The number of days after a password expires to lock the account (INACTIVE; 0 = immediate, 99999 = never):	99999

Failed Login Response

This section allows you to modify the failed login response policy.
Changes to these parameters take effect immediately on submittal of this page.

☑ Enable account lock out parameters (PAM Tally)

Lock out account after the following number of unsuccessful attempts (DENY): 5

Automatically unlock a locked account after the following number of seconds (UNLOCK_TIME): 600

Reset the failed attempt counter after last failed attempt (UNLOCK_RESET): ● yes ○ no

© 2001-2010 Avaya Inc. All Rights Reserved.

Table 23: Login Account Policy fields and parameters

Field	Parameters
Credential Expiration Parameters	
The maximum number of days a password may be used (PASS_MAX_DAYS):	1-99999
The minimum number of days allowed between password changes (PASS_MIN_DAYS):	0-99999
The number of days a warning is given before a password expires (PASS_WARN_AGE):	0-30
The number of days after a password expires to lock the account (INACTIVE, 0= immediate, 99999=never):	0-99999 **Note:** 0 = immediate 99999 = never
Failed Login Response	
Enable account lock out parameters (PAM Tally)	If not checked, the remaining parameters (below) are ignored.
Lock out account after the following number of unsuccessful attempts (DENY):	1-9
Automatically unlock a locked account after the following number of seconds (UNLOCK_TIME):	1-99999
Reset the failed attempt counter after last failed attempt (UNLOCK_RESET):	Yes or No

For more information on password management, credentials expiration and lockout policies for branch gateways, see:

- *Administration for the Avaya G250 and Avaya G350 Media Gateways,* (03-300436)
- *Administration for the Avaya G430 Media Gateway*, (03-603228)
- *Administration for the Avaya G450 Media Gateway*, (03-602055)

Password administration recommendations

For Communication Manager password management, take into account the following recommendations and constraints:

- Because system access by Avaya Services is infrequent yet often required to maintain maximum uptime, do not enable password aging for Avaya services accounts.
- Use care in enabling password aging for accounts authenticated through external servers, for example RADIUS accounts, that do not support the user changing a password through the Communication Manager server. If such a user's account expires, PAM issues a prompt to change the password. If this is not possible through Communication Manager, then this user is locked out.

Credentials management

Credentials (usernames and passwords) for standard Linux accounts in Communication Manager are stored in `/etc/passwd`, `/etc/shadow`, and `/etc/group`, plus the backup files for those files, for example, `/etc/group-` and `/etc/passwd-`.

Communication Manager does not use a database to store credentials information.

- Passwords for local accounts are stored in /etc/shadow. Passwords in /etc/shadow are stored as a one-way hash. The file `/etc/shadow` is root restricted.
- Usernames and group membership for local Communication Manager accounts can be viewed by any user logged into Linux.
- ASG accounts have additional information stored in files that are AES encrypted.
- Credentials configured for an external AAA server such as RADIUS or LDAP are stored in the external server, not within Communication Manager.

More information

- Avaya's encryption overview on page 43

Applying profiles for role-based administration

Role based access control (RBAC) allows businesses to assign server, gateway, and application access permissions based on a user's job function, or role. Avaya implements RBAC to the Communication Manager Server through the use of profiles for both the Server web page and SAT interfaces.

Avaya customers can create and modify profiles to allow access to Avaya server and gateway information according to job functions and business needs. Table 24: RBAC profile examples on page 104 lists examples.

Table 24: RBAC profile examples

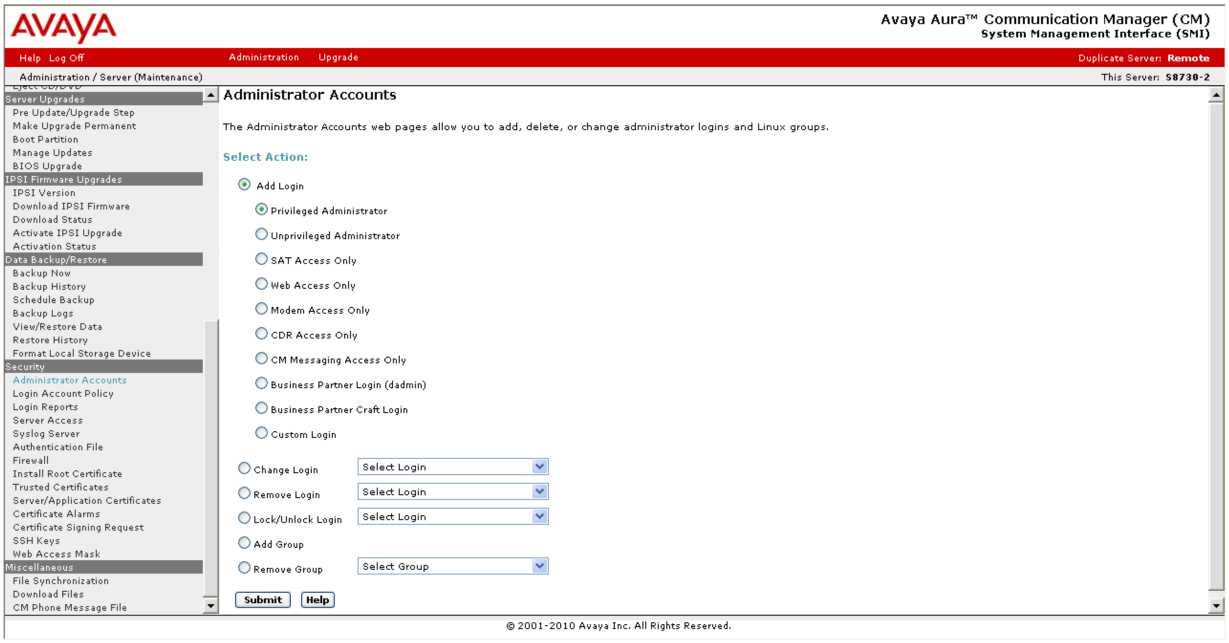
Profile name	Job function and access permissions
Privileged Administrator	This login has the greatest access in the system with the exception of the "root" login: read-write access to system parameters (for example, IP addresses, upgrade software), modify, assign, or define other roles, and read/write access to create and modify logins. See Creating the privileged administrator account on page 105 for procedures to set up this account.
Backup Administrator	Ability to perform only backups and restores.
Security Administrator	Read-write access to create other logins; create, modify or assign roles and profiles; install ASG keys, install licenses, install PKI certificates and keys.
Avaya Maintenance and Support	Access to maintenance logs, run diagnostics.
Auditor	Read-only access to logs and audit files. Read-only permissions prevents unauthorized modification of log files.
Telephony Application Administrator	Read-write access to application configuration, such as trunks
Telephone Provisioning	Ability to add, change, and delete a certain range of telephone extensions
ACD Administrator	Ability to modify call center vectors
Checker	Read-only access, able to only view certain changes

Creating the privileged administrator account

Use this section to create the privileged administrator account, which has the highest level access in the system (except “root”).

1. At the System Management Interface select **Security > Administrator Accounts**.

Figure 8: Communication Manager Administrator Accounts page



Administrator Accounts

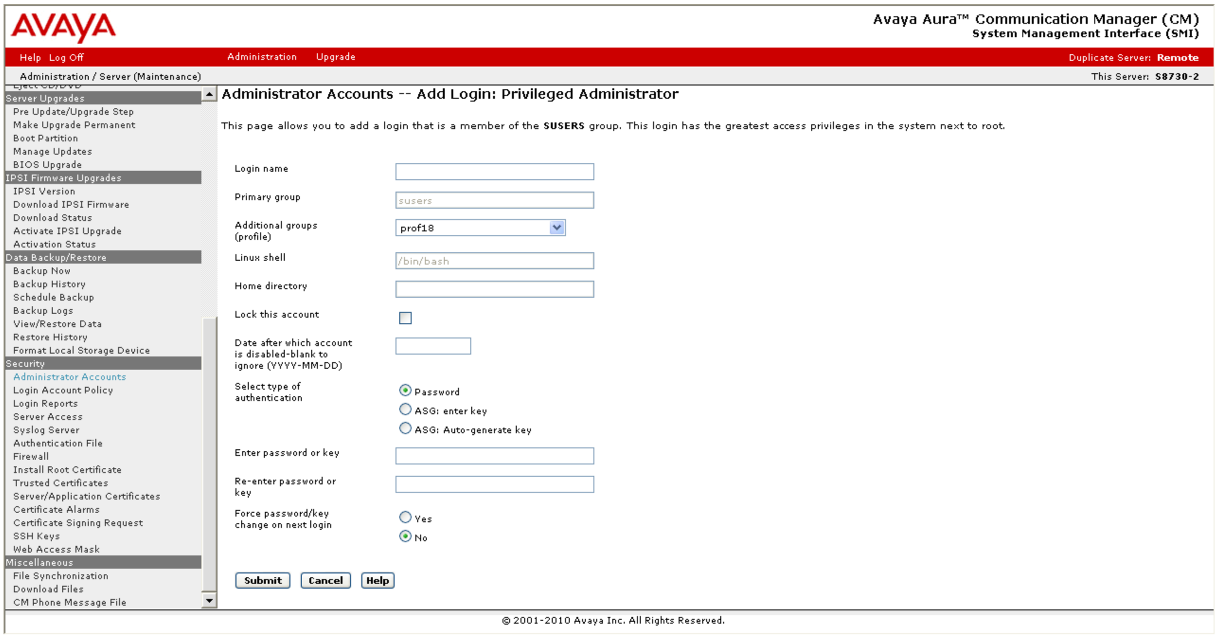
The Administrator Accounts web pages allow you to add, delete, or change administrator logins and Linux groups.

Select Action:

- ● Add Login
  - ● Privileged Administrator
  - ○ Unprivileged Administrator
  - ○ SAT Access Only
  - ○ Web Access Only
  - ○ Modem Access Only
  - ○ CDR Access Only
  - ○ CM Messaging Access Only
  - ○ Business Partner Login (dadmin)
  - ○ Business Partner Craft Login
  - ○ Custom Login
- ○ Change Login — Select Login
- ○ Remove Login — Select Login
- ○ Lock/Unlock Login — Select Login
- ○ Add Group
- ○ Remove Group — Select Group

2. Select **Add Login** and **Privileged Administrator**, click **Submit**.
   The system displays the **Administrator Accounts -- Add Login: Privileged Administrator** page.

Figure 9: Administrator Accounts -- Add Login: Privileged Administrator page



Administrator Accounts -- Add Login: Privileged Administrator

This page allows you to add a login that is a member of the **SUSERS** group. This login has the greatest access privileges in the system next to root.

Login name	
Primary group	susers
Additional groups (profile)	prof18
Linux shell	/bin/bash
Home directory	
Lock this account	□
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	
Select type of authentication	● Password ○ ASG: enter key ○ ASG: Auto-generate key
Enter password or key	
Re-enter password or key	
Force password/key change on next login	○ Yes ● No

3. Use Table 25: Administrator Accounts -- Add Login: Privileged Administrator field descriptions and values on page 106, to fill in the appropriate fields.

Table 25: Administrator Accounts -- Add Login: Privileged Administrator field descriptions and values

Field	Description / Values
Login name	Up to 31 characters (a-z, A-Z, 0-9). The login name cannot already exist or cannot be a protected login name. New or modified ASG customer protected logins requires an AES key.
Primary group	Set to `susers` and cannot be changed.
Additional groups	Drop-down menu contains profiles 18 (default) through 69.
	1 of 4

Table 25: Administrator Accounts -- Add Login: Privileged Administrator field descriptions and values

Field	Description / Values
Linux shell	Set to `/bin/bash` and cannot be changed.
Home directory	Updated automatically to `/var/home/`*`login-name`* when the **Login name** field is populated. The entry cannot be changed.
Lock this account	Select this checkbox if you want to lock the user from logging into the system. (Optional)
Date to disable	Enter a date when the login should be disabled in the *yyyy-mm-dd* format or blank (never disabled).
Type of authentication	● Password ● ASG: enter key (user defined, ASG user information must include the ASG key) ● ASG: Auto-generate key (CM automatically generates the ASG key) ⚠ **WARNING:** Selecting this button deactivates the **Enter key or password** and **Re-enter key or password** fields.
	2 of 4

Table 25: Administrator Accounts -- Add Login: Privileged Administrator field descriptions and values

Field	Description / Values
Enter key or password	Field can be up to 31 characters, and can include the following: ● lowercase letters of the English alphabet (a-z) ● uppercase or capital letters of the English alphabet (A-Z) ● 0-9 ● periods (.) ● hyphens (-) ● underscores (_) ● dollar sign ($) ● a blank space ● colons (:) ● semi-colons (;) ● commas (,) ● equal sign (=) ● forward slash (/) ● ampersand (&) ● pound sign (#) ● plus sign (+) ● apostrophe (’) ● asterisk (*) ● quotation marks (" ") ● parentheses(()) Prior to Communication Manager 6.0, the ASG key must be exactly 20 digits. Each digit must be an octal number, that is, between 0-7. The last digit must be zero ("0”) and the penultimate digit must be an even number. From Communication Manager 6.0 onwards the ASG key are AES encrypted with a 32 digit key with hexadecimal characters.
	3 of 4

Table 25: Administrator Accounts -- Add Login: Privileged Administrator field descriptions and values

Field	Description / Values
Re-enter key or password	Enter the password or key to exactly match the **Enter key or password** field (required if **Authentication** is **Password** or **ASG**.
Force password/key change on first login	Select **Yes** (requires password change on first use) or **No**.
	4 of 4

More information

For information on administering profiles, see:

- http://support.avaya.com to view and download the *Communication Manager Administrator Logins White Paper*.
- http://support.avaya.com to download the *Documentation for Avaya Commmunication Manager, Media Gateways and Servers* CD, and the individual documents:
    - *Administering Avaya Aura™ Communication Manager (03-300509)*
    - *Avaya Aura™ Communication Manager Feature Description and Implementation (555-245-205)*
    - *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers (03-300431)*
    - Administration for the Avaya G430 Media Gateway, (03-603228)
    - Administration for the Avaya G450 Media Gateway, (03-602055)

Managing administrative accounts

Avaya provides authentication and access control to both the Communication Manager System Management Interface and the SAT interface.

Detailed access control is administered through the interfaces as described in Table 26: Managing Communication Manager accounts on page 110. In addition, see *Avaya Aura™ Communication Manager Feature Description and Implementation (555-245-205).*

Table 26: Managing Communication Manager accounts

Communication Manager account administration	Interface
Managing Avaya Server web interface login accounts ● Adding an administrator account (login) ● Changing, locking, removing logins ● Adding and removing login groups	System Management Interface **Security>Administrator Accounts**
Managing Avaya server web access profiles ● Adding web access profiles ● Changing, duplicating, and deleting web profiles	System Management Interface **Security>Web Access Mask**
Managing passwords and Access Security Gateway (ASG)	System Management Interface **Security>Web Access Mask**
Managing profiles for SAT interface access ● Adding a user profile for using the SAT ● Adding extended profiles ● Duplicating and deleting SAT profiles	SAT Screen **User Profile**

Account administration recommendations

For Communication Manager login account management, take into account the following recommendations and constraints:

- Administer at least one local host account in all servers so that access is possible even if external AAA servers are not reachable.
- All ASG authenticated accounts must be local host accounts. A PAM module to support ASG authentication through an external server does not exist.
- Because system access by Avaya Services is infrequent yet often required to maintain maximum uptime, do not enable password aging for Avaya Services accounts.
- Use RADIUS, RSA SecurID, and SafeWord AAA services in conjunction with a parallel local host account or LDAP/NSS. When configuring a local host account, lock the local account to prevent a stale local password from being used in the event that the external AAA server is not reachable.
- Simple Authentication and Security Layer (SASL) authentication is not supported.

Administering authentication passwords

Passwords for Communication Manager servers are administered on System Management Interface, where individual login password parameters are established for:

- Type of access shell: standard, CDR or remote
- Type of authentication: password or Access Security Gateway (ASG)
- Management parameters: expiration, change, and lock rules

Set login and password parameters on the **Administrator Logins -- Add Login** page as described in *Avaya Aura™ Communication Manager Feature Description and Implementation (555-245-205)*.

Access Security Gateway (ASG)

Access Security Gateway (ASG) is a software feature available on most Avaya products and uses challenge/responses for authentication by associating a unique secret key with each login on every product. When products are installed, an Avaya security management system called the ASG Manager creates new ASG encryption keys for each Avaya login on every system. Every Avaya login on an Avaya system is associated with a different key. If a key were ever compromised, only a single login on a single system would be affected. The encryption keys are themselves encrypted before they are installed. ASG is session-oriented. A unique challenge is presented, and a unique response must be provided each time the user wants to be authenticated by the Avaya system. ASG uses Advanced Encryption Standard (128-bit AES key) technology.

Communication Manager provides the ASG process, which is used for Avaya Services login accounts and can be assigned to customer-created administrator logins. ASG replaces static password authentication and adds a level of security to system administration and maintenance ports and/or logins on Communication Manager. Avaya support (services) accounts are protected by ASG. Customer logins may use ASG if it is enabled in the system license.

A regular password account uses a fixed user name (ID) and a password that can be used multiple times to log into the system. A person or device that can monitor (network sniffer) the login messages can capture this password and use it to gain access. ASG instead uses a one-time challenge-response mechanism to authenticate users. The user is allowed to log in only when the correct response is entered. The password is unique to that session and is incorrect if used again. Even if the password is compromised, it cannot be re-used immediately or at a later time, even by the same person from the same terminal. ASG can be enabled on the System Management Interface for each login on an Avaya server if the feature is enabled in the system license.

ASG Guard and ASG Guard Plus

The ASG Guard is an outboard appliance providing access security for Avaya products that do not have ASG software as a native application. It supports 4 to 28 console ports (achieved through optional expansion boards) and secures physically-connected devices through serial interfaces. ASG Guard has over 30Mb of memory to store keystroke logging of administrative sessions and can transfer the data to the (optional) ASG Guardian for centralized storage and viewing. Such information can provide the foundation for routine operational reviews and post-breach analysis.

The ASG Guard is accessed over dial-up connections from the ASG Guardian Portal through encrypted dial-up, offering features such as single sign-on, multi-factor authentication, and definition of security policies, and delivers a scalable and auditable gateway for all administrative class users. The ASG Guard capabilities help protect distributed corporate networks from malicious, administrative channel attacks from a “trusted” third-party vendor or simple, inexperienced user error from an internal administrator.

The ASG Guard has four (4) product connection ports. The ASG Guard Plus has sixteen (16) ports, or twenty-eight (28) ports using the expansion module. The ASG Guard or Guard Plus is used as the only remote access point into the maintenance and administrative ports of the protected products. The ASG Guard or Guard Plus provide a seven (7) digit unique challenge when accessed, and once the correct response has been received, the user can then access the protected product. If the user reaches the protected product, any access requirements of the product, such as passwords, remain the same.

ASG Guard II

Avaya’s ASG Guard II supports 4 console ports that enable security of physically-connected devices through serial interfaces and 16 logical IP ports. By utilizing integrated VPN Firewall router functionality, the ASG Guard II is also able to protect administrative access points on up to 16 IP-enabled devices. Therefore, in a VoIP environment administrator-level users can access only those devices to which they have been granted privileges.

ASG Guard and ASG Guard II compared

Table 27: Comparative features: ASG Guard and ASG Guard II on page 114 lists and compares the features of ASG Guard and ASG Guard II.

Table 27: Comparative features: ASG Guard and ASG Guard II

Features	ASG Guard	ASG Guard II
Number of unit logins	75	200
Single DES authentication	Y	Y
3 DES (Avaya infrastructure currently supports DES)	Y	Y
RSA Secure ID Compatibility	Y (with ASG Guardian)	Y (with ASG Guardian)
Encrypted Keys/password	Y	Y
Import/Export of users	Y	Y
Tamper Proof logs	Y	Y
Access history log	Y	Y
Failure history log	Y	Y
Failed authentication alarms	Y	Y
Session buffer	Y	Y
Encrypted connection (IPSec, SSH)	N	Y
Segregate management access from enterprise network	N	Y
Deny/Allow Command	Y	Y
Environmental monitoring (temperature and contact closures)	Y	Y
Phone line consolidation	Y	Y
Collaborative sessions	Y	Y

ASG security products

Additional ASG security products that provide further access security options are available. Documentation regarding the Access Security Gateway family of security products is online at http://support.avaya.com/japple/css/japple?PAGE=Product&temp.productID=107697.

Toll fraud prevention

Limiting long distance access

Avaya Toll Fraud and Security Handbook (555-025-600) contains several topics with information about limiting unauthorized calls:

- "Tools that restrict unauthorized outgoing calls" in Chapter 5 discusses several ways to avoid toll-fraud:
  - Class of Restriction (COR) administration
  - Facility restrictions
  - AAR/ARS analysis
  - Restrictions on station permissions, central office, and incoming tie trunks
- "Security measures" in Chapter 5 recommends many ways in which unauthorized use is restricted:
  - Administer Facility Restriction Levels (FRLs)
  - Prevent after-hours calling with Time-of-Day Routing
  - Limiting/blocking international calling
  - Restricting/allowing calls to specified area codes/numbers
  - Assigning Class of Restriction (COR)
  - Trunk access and transfer restrictions
- "Detecting toll fraud" in Chapter 5 details how to monitor for toll fraud:
  - Traffic measurements and performance
  - Call Management System (CMS) measurements
  - Security Violations Measurements reports
  - Malicious call trace
  - Service observing
  - Call-forwarding command

Configuring logging and events

- Configuring SNMP and syslog on page 116

Configuring SNMP and syslog

You can receive event notifications and interactive data from the entire Avaya enterprise - main server and Communication Manager, messaging and other telephony applications, gateways, and endpoints - through logs, through SNMP, or both.

All syslog files are found under a sub-directory of the `/var/log/cmm directory`. The first level sub-directory is a major component of CMM and contains the security syslogs for that component, for example, `/var/log/cmm/iim/security.log`.

What security-related events are logged?

Security events are related to the following actions or activities:

- Attempted login or log off, whether successful or not
- Establishment of a new administrative access session regardless of port of entry
- Assignment of a user profile to an administrative session
- Display, list, change, add or delete of a user profile
- Any administrative access to local user accounts (view, add, change, delete)
- Failed attempt to access an object or execute an action to which the user does not have access
- Any access to the security control configuration of the server: logging configuration, the PAM configuration, or the firewall configuration.

Note:
You cannot disable logging of security events.

Table 28: Logging facility and priority for security and non-security events on page 117 shows the syslog priority and facility for security and non-security events.

Table 28: Logging facility and priority for security and non-security events

Type of event	Example	Priority	Facility
Security	successful login	notice	auth or priv
	failed login	alert	
Non-security		notice	local0
SNMP			local0

Depending on your logging or notification requirements, use the following sections to configure security events notifications:

- Configuring SNMP in Communication Manager on page 118
- Configuring the syslog server in Communication Manager on page 123
- Accessing system logs through the Web on page 129 provides another way to select, filter and view the syslog through the Communication Manager System Management Interface.
- Restricting web access to system logs on page 169 has information on how to assign or restrict user access privileges to the syslog.

Configuring SNMP in Communication Manager

The SNMP protocol provides a simple set of operations that allow remote management of devices in a network.

Communication Manager supports the following SNMP versions:

- SNMP Version 1 (SNMP v1) and SNMP Version 2c (SNMP v2c): based on plain-text strings known as communities which are passwords that allow any SNMP-based application access to a device’s management information.
- SNMP Version 3 (SNMP v3) provides secure authentication and communication between managed entities.

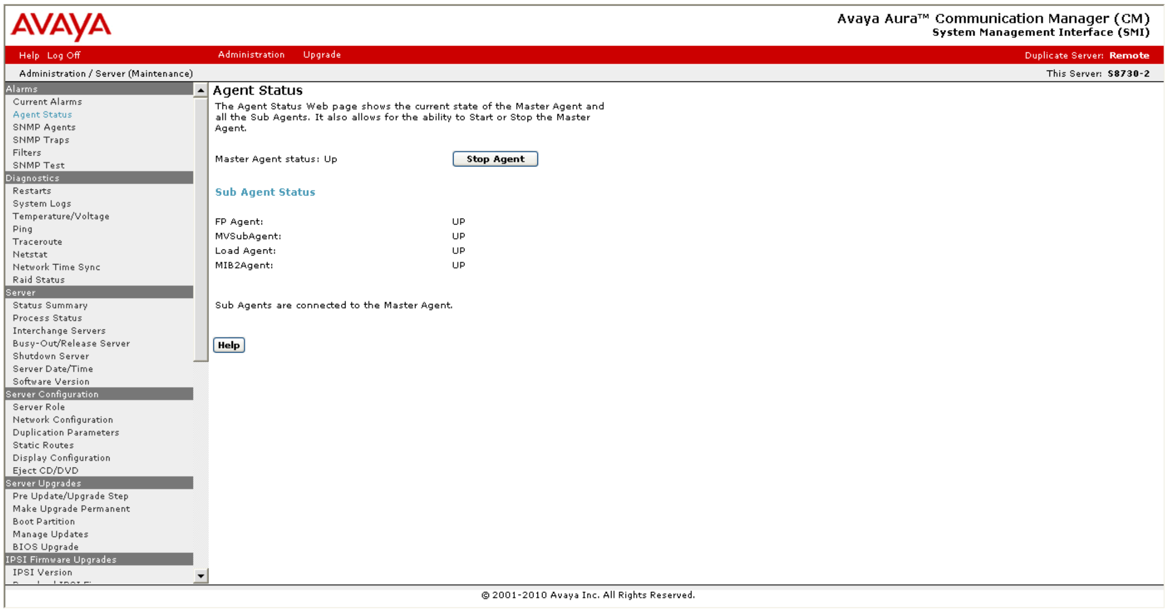
Configure SNMP through these Communication Manager System Management Interface:

- Agent Status page on page 119
- SNMP Agents page on page 119
- SNMP Traps page on page 121 and SNMP Traps (Add Trap Destination) page on page 122

Agent Status page

The order in which you set up SNMP is important. First, disable the SNMP agent at the Communication Manager System Management Interface (**Alarms > Agent Status** on the left-side navigation pane, and shown in Figure 10: Agent Status page on page 119).

Figure 10: Agent Status page



Agent Status

The Agent Status Web page shows the current state of the Master Agent and all the Sub Agents. It also allows for the ability to Start or Stop the Master Agent.

Master Agent status: Up

Sub Agent Status

FP Agent: UP
MVSubAgent: UP
Load Agent: UP
MIB2Agent: UP

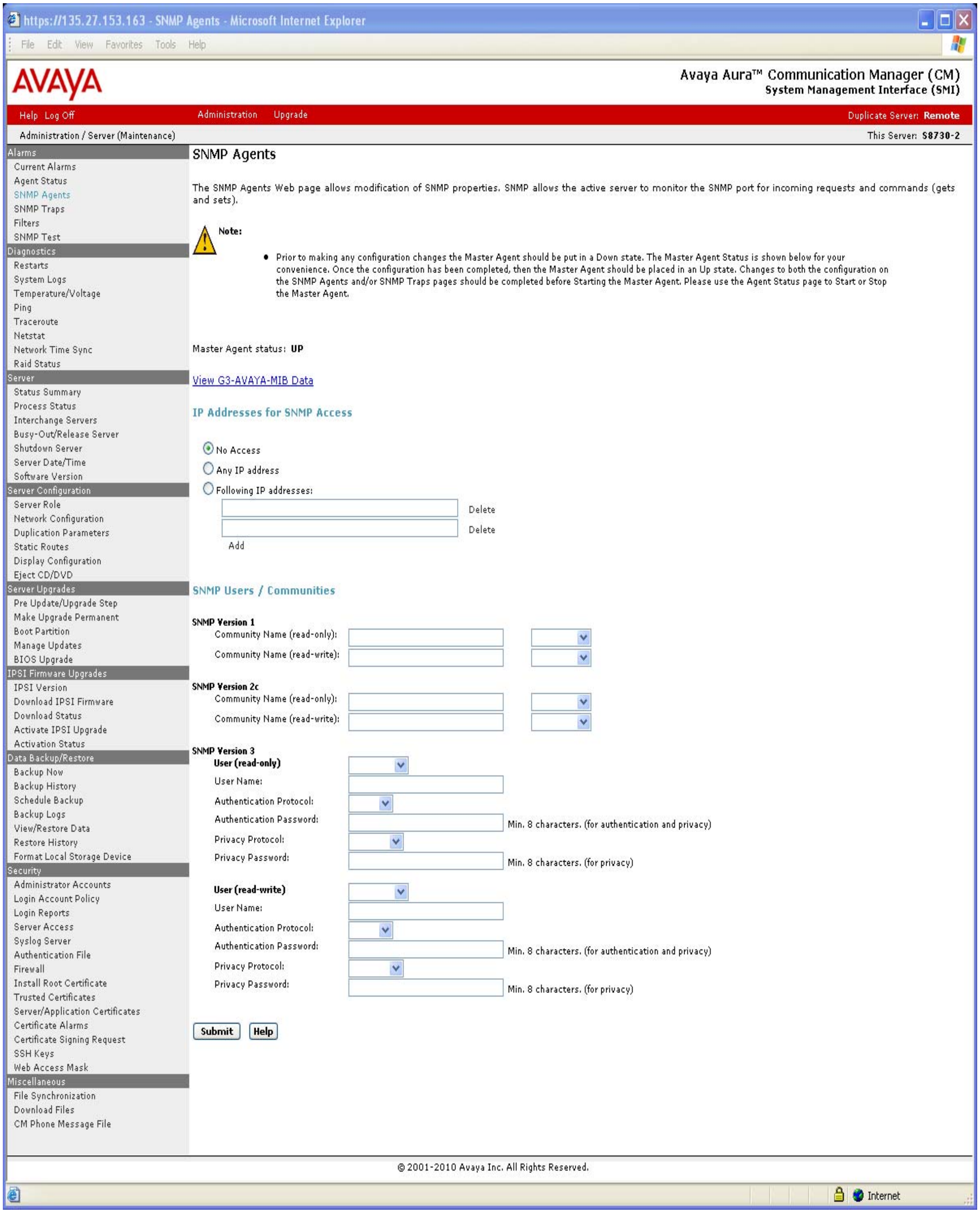
Sub Agents are connected to the Master Agent.

SNMP Agents page

Configure the SNMP agent through the Communication Manager System Management Interface (**Alarms > SNMP Agents** on the left-side navigation pane, as shown in Figure 11: SNMP Agents page on page 120).

Note:
SNMP agents always log user activity; you cannot enable or disable this logging.

Figure 11: SNMP Agents page



SNMP Agents

The SNMP Agents Web page allows modification of SNMP properties. SNMP allows the active server to monitor the SNMP port for incoming requests and commands (gets and sets).

Note:

- Prior to making any configuration changes the Master Agent should be put in a Down state. The Master Agent Status is shown below for your convenience. Once the configuration has been completed, then the Master Agent should be placed in an Up state. Changes to both the configuration on the SNMP Agents and/or SNMP Traps pages should be completed before Starting the Master Agent. Please use the Agent Status page to Start or Stop the Master Agent.

Master Agent status: **UP**

View G3-AVAYA-MIB Data

IP Addresses for SNMP Access

● No Access
○ Any IP address
○ Following IP addresses:
[ ] Delete
[ ] Delete
Add

SNMP Users / Communities

SNMP Version 1
Community Name (read-only):
Community Name (read-write):

SNMP Version 2c
Community Name (read-only):
Community Name (read-write):

SNMP Version 3
User (read-only)
User Name:
Authentication Protocol:
Authentication Password: Min. 8 characters. (for authentication and privacy)
Privacy Protocol:
Privacy Password: Min. 8 characters. (for privacy)

User (read-write)
User Name:
Authentication Protocol:
Authentication Password: Min. 8 characters. (for authentication and privacy)
Privacy Protocol:
Privacy Password: Min. 8 characters. (for privacy)

Submit Help

© 2001-2010 Avaya Inc. All Rights Reserved.

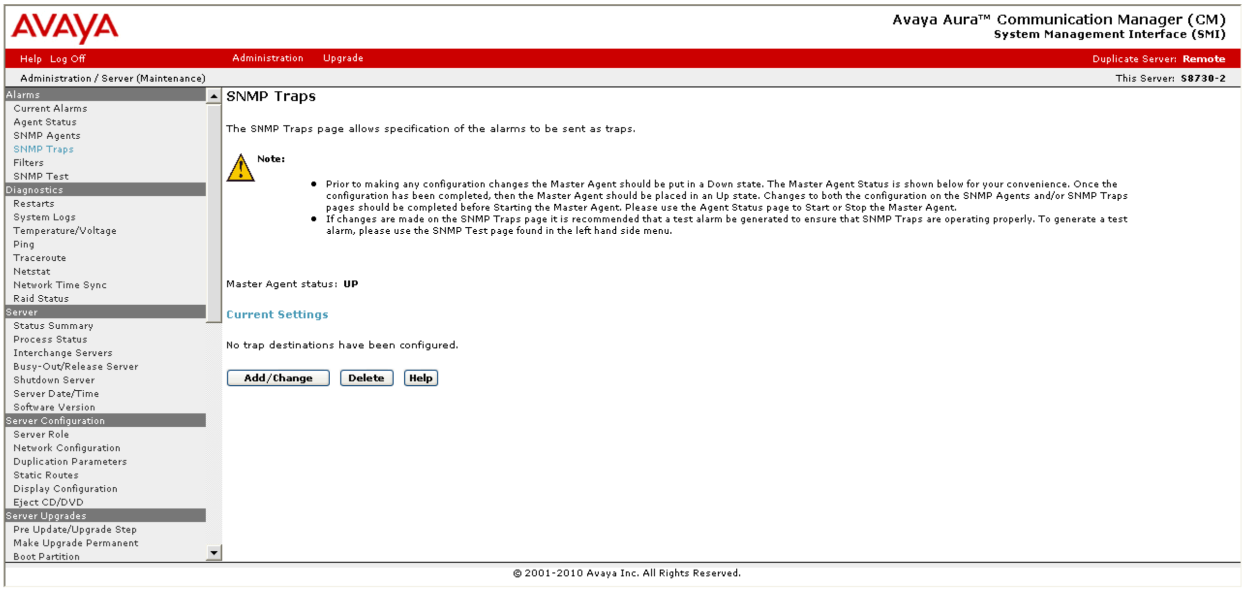
This **SNMP Agents** page allows you to:

- Block access to the SNMP port
- Monitor the SNMP port for incoming requests and commands (gets and sets) from specified IP address or any IP address
- Enable SNMP v1, v2, or v3

SNMP Traps page

The **SNMP Traps** page (see Figure 12: SNMP Traps page on page 121) allows you to specify which alarms are set as traps.

Figure 12: SNMP Traps page



SNMP Traps

The SNMP Traps page allows specification of the alarms to be sent as traps.

Note:

- Prior to making any configuration changes the Master Agent should be put in a Down state. The Master Agent Status is shown below for your convenience. Once the configuration has been completed, then the Master Agent should be placed in an Up state. Changes to both the configuration on the SNMP Agents and/or SNMP Traps pages should be completed before Starting the Master Agent. Please use the Agent Status page to Start or Stop the Master Agent.
- If changes are made on the SNMP Traps page it is recommended that a test alarm be generated to ensure that SNMP Traps are operating properly. To generate a test alarm, please use the SNMP Test page found in the left hand side menu.

Master Agent status: **UP**

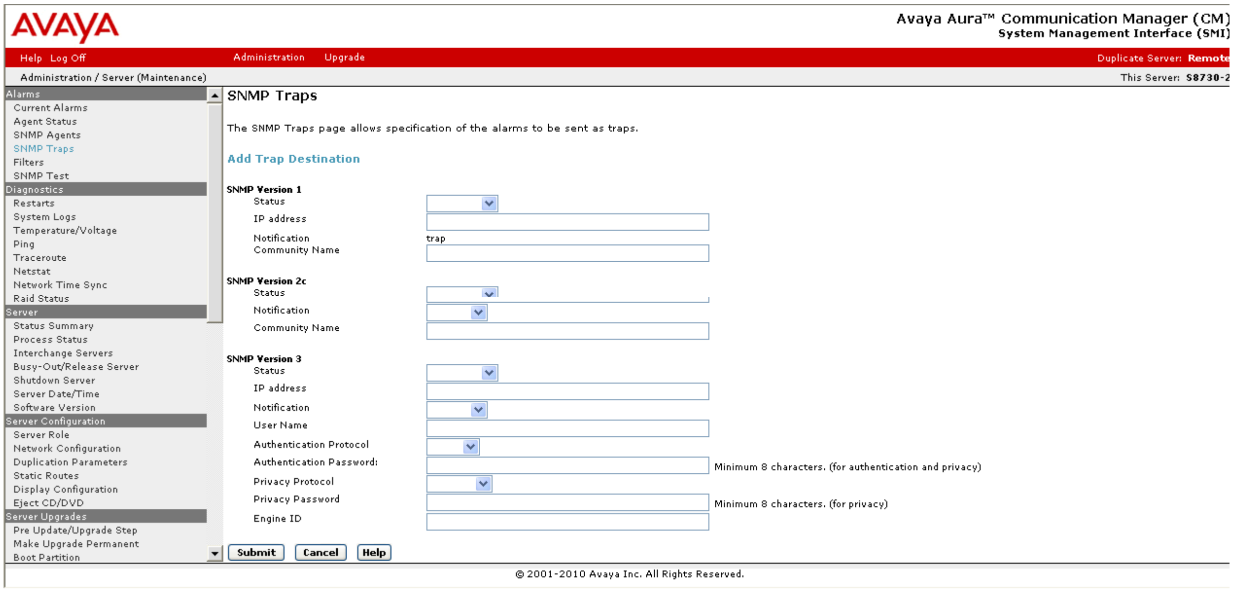
Current Settings

No trap destinations have been configured.

© 2001-2010 Avaya Inc. All Rights Reserved.

Clicking **Add/Change** allows you to administer alarm traps and their destinations from the **SNMP Traps (Add Trap Destination)** page, as shown in Figure 13: SNMP Traps (Add Trap Destination) page on page 122.

Figure 13: SNMP Traps (Add Trap Destination) page



SNMP Traps

The SNMP Traps page allows specification of the alarms to be sent as traps.

Add Trap Destination

SNMP Version 1

Status

IP address

Notification Community Name: trap

SNMP Version 2c

Status

Notification

Community Name

SNMP Version 3

Status

IP address

Notification

User Name

Authentication Protocol

Authentication Password: Minimum 8 characters. (for authentication and privacy)

Privacy Protocol

Privacy Password: Minimum 8 characters. (for privacy)

Engine ID

© 2001-2010 Avaya Inc. All Rights Reserved.

The highest SNMP protocol, version 3, is the most secure and allows three (3) security levels (**Security Model** field):

- **None**: traps are sent in plain text without a digital certificate.
- **Authentication**: an authentication password is required. SNMP v3 uses this pass phrase to digitally "sign" v3 traps using MD5 protocol to associate the traps with the user.
- **Privacy**: both an authentication password and a privacy password are required for user-specific authentication and encryption. Traps are signed and encrypted using Data Encryption Standard (DES) protocol.

Re-enable SNMP agent

To complete setting up SNMP notifications, go to the Agent Status page on page 119 and re-enable the SNMP agent.

Communication Manager security event notifications through SNMP

SNMP Reference Guide for Avaya Communication Manager (03-602013) lists the types of security-related trap notifications that SNMP can deliver to a trap receiver and/ or to Avaya's Initialization and Administration System (INADS) monitoring through Avaya Services.

Note:
SNMP agents log access that changes values or initiates actions (for example "set" commands) to any object or command outside of Communication Manager. For example, SNMP agents do not log these Communication Manager activities:

- IPSI downloads and resets
- Communication Manager platform upgrades (update script)

For information on Configuring SNMP traps for branch gateways, see:

- Chapter 13 of *Administration for the Avaya G250 and Avaya G350 Media Gateways,* (03-300436)
- Chapter 13 of *Administration for the Avaya G430 Media Gateway*, (03-603228)
- Chapter 13 of *Administration for the Avaya G450 Media Gateway*, (03-602055)

Configuring the syslog server in Communication Manager

The syslog is stored locally on the server but can be exported to an external server:

- Avaya maintains a local syslog on the server to facilitate debugging, regardless of whether the customer chooses to log information to an external server.
- Customers need to send parts or all of the log information to an external server in real time for a variety of reasons.

The syslog service allows customers to send data from certain logs or log groups to an external server without disturbing Avaya's method for saving logs locally.

Topics in this section include:

- General syslog guidelines on page 124 details what syslog contains, file synchronization options, and firewall activity for the syslog server.
- Administering the syslog server in Communication Manager on page 125 helps you configure the Communication Manager syslog server.
- In case you do not want to see log entries for every event, how to filter or select the information that is delivered to the syslog is in Administering logging levels in Communication Manager on page 126.

General syslog guidelines

- Logging to an external syslog server is disabled by default, however Avaya maintains a local log, regardless of whether logging to an external is enabled or not.
- Syslog always logs security violation events which cannot disable this logging through administration.
- Old/new values are logged according to administration on the logging levels form (see Figure 15: Logging Levels form, page 1 of 2 on page 126).
- You can enable logging to one external server only. Configuration parameters for the external syslog server are added to the `/etc/syslog.conf` file. If you disable sending these events, the configuration parameters are removed from `syslog.conf` file.
- You can synchronize the `syslog.conf` file to the standby server and all ESS/LSP servers.
- The external syslog server configuration is saved as part of the security backup data set.
- The server firewall automatically opens outbound for the syslog port (514 UDP) if the user enables logging to an external syslog server and automatically closes if logging is not enabled.

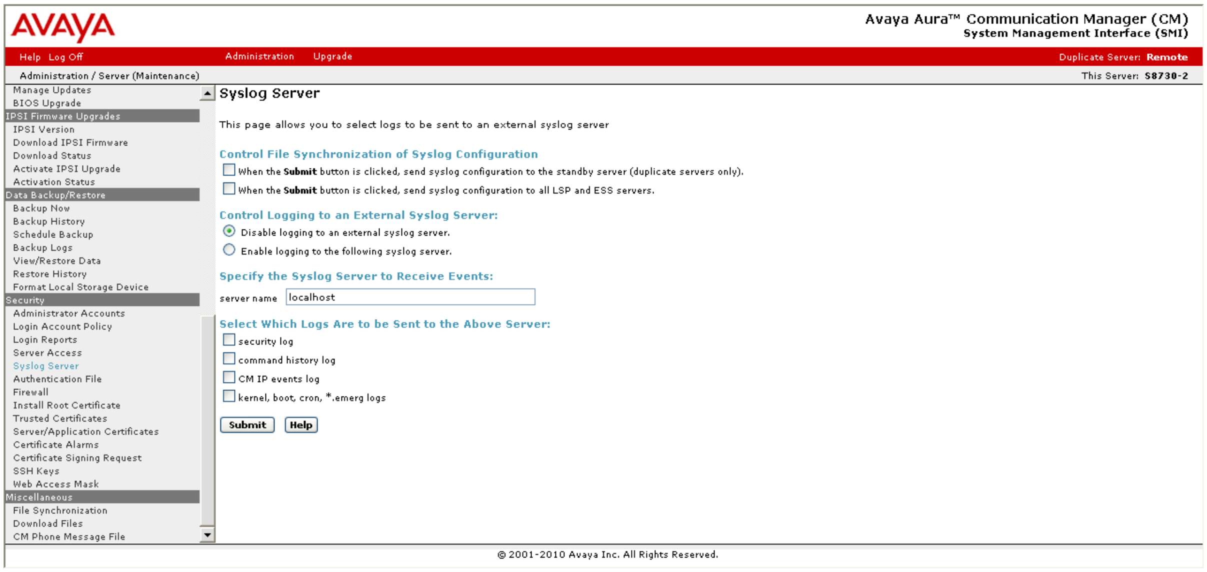
Administering the syslog server in Communication Manager

Note:

Logging to an external syslog server is disabled by default in Communication Manager.

The Communication Manager System Management Interface (**Security > Syslog Server** on the left-side navigation pane) displays **Syslog Server** page (Figure 14: Syslog Server page on page 125).

Figure 14: Syslog Server page



Syslog Server

This page allows you to select logs to be sent to an external syslog server

Control File Synchronization of Syslog Configuration

□ When the **Submit** button is clicked, send syslog configuration to the standby server (duplicate servers only).

□ When the **Submit** button is clicked, send syslog configuration to all LSP and ESS servers.

Control Logging to an External Syslog Server:

● Disable logging to an external syslog server.

○ Enable logging to the following syslog server.

Specify the Syslog Server to Receive Events:

server name localhost

Select Which Logs Are to be Sent to the Above Server:

□ security log

□ command history log

□ CM IP events log

□ kernel, boot, cron, *.emerg logs

© 2001-2010 Avaya Inc. All Rights Reserved.

The **Syslog Server** page permits the following functions:

- **Control File Synchronization of Syslog Configuration** gives you the option to synchronize the syslog configuration file with a standby or LSP/ESS server:
  - Check **Synchronize syslog configuration to the standby server (duplicated servers)** if you want to synchronize the main server's syslog configuration to the standby server.
  - Check **Synchronize syslog configuration to all LSP and ESS servers** if you want to synchronize the main server's syslog configuration to any administered LSP/ESS server(s).

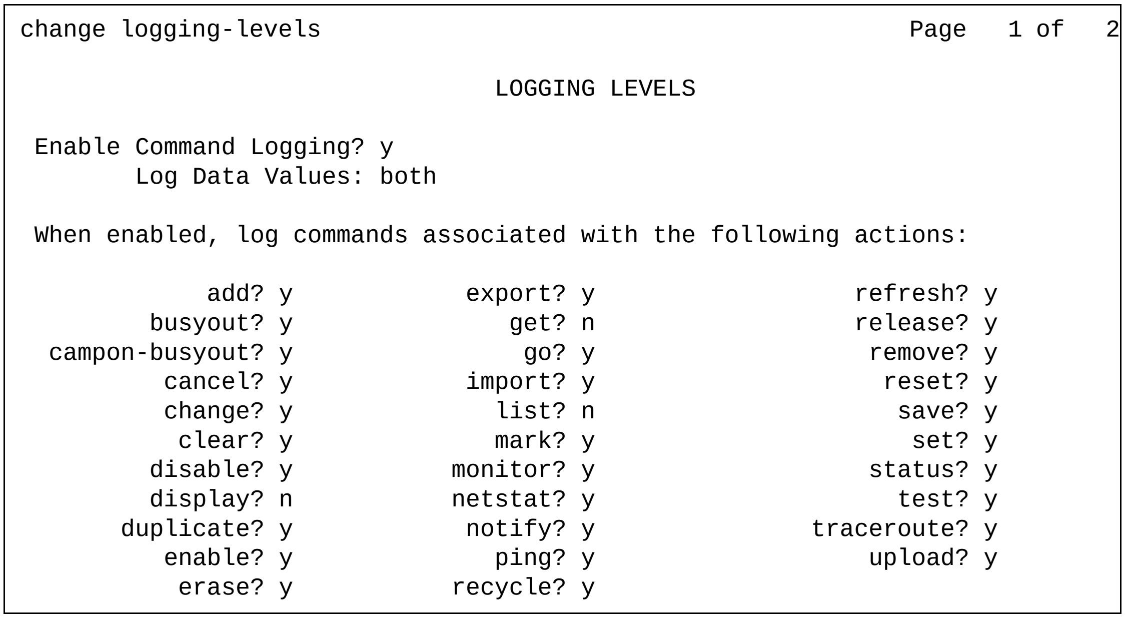
- The **Select Which Logs Are to be Sent to the Above Server** section allows you to select the logs that you want to send to the external syslog server:
  - Security log (`var/log/secure`)
  - Command history log (`var/log/ecs/command history`)
  - Communication Manager IP events log (`/var/log/messages`)
  - kernel, boot, cron, *`*.info`*, *`*.emerg`* logs (`/var/log/messages`)

Administering logging levels in Communication Manager

You can select only the activities that you want to monitor by administering the **Logging Levels** form (Figure 15: Logging Levels form, page 1 of 2 on page 126) in Communication Manager.

Note:
The defaults in Communication Manager's **Logging Levels** form produce the same amount and type of logging as Communication Manager releases prior to Release 4.0.

Figure 15: Logging Levels form, page 1 of 2



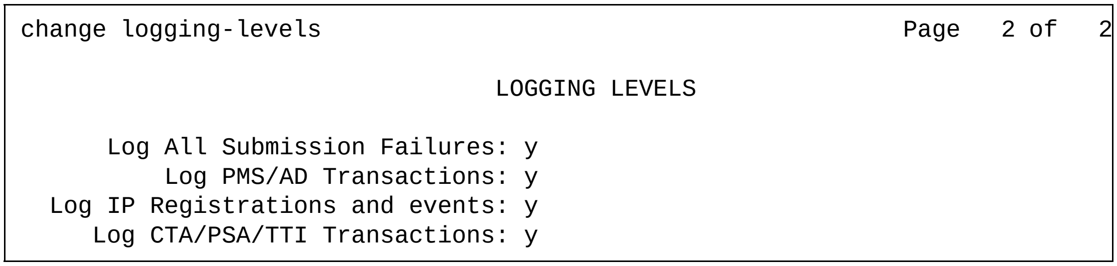
```
change logging-levels                                           Page   1 of   2

                                  LOGGING LEVELS

 Enable Command Logging? y
        Log Data Values: both

 When enabled, log commands associated with the following actions:

             add? y            export? y                   refresh? y
         busyout? y               get? n                   release? y
  campon-busyout? y                go? y                    remove? y
          cancel? y            import? y                     reset? y
          change? y              list? n                      save? y
           clear? y              mark? y                       set? y
         disable? y           monitor? y                    status? y
         display? n           netstat? y                      test? y
       duplicate? y            notify? y                traceroute? y
          enable? y              ping? y                    upload? y
           erase? y           recycle? y
```

Table 29: Logging Level form, page 1 of 2 fields and descriptions

Field	Values	Description
Enable Command Logging	**no**	SAT activity is not logged.
	yes	SAT activity is logged based on the selections on the **Logging Levels** form.
Log Data Values	**none**	Only the object, the qualifier, and the command action are logged.
	new	Only the new value of any field is logged; the old value is not logged.
	both	Both the field value prior to the change and the field value after the change are logged.
When enabled, log commands associated with the following actions	**y**(es)	Creates a log entry for this action.
	n(o)	Does not create a log entry for this action.

The second page of the form (Figure 16: Logging Levels form, page 2 of 2 on page 127) allows further refinement of the information that is delivered to the syslog.

Figure 16: Logging Levels form, page 2 of 2



```
change logging-levels                                       Page   2 of   2

                                 LOGGING LEVELS

      Log All Submission Failures: y
          Log PMS/AD Transactions: y
  Log IP Registrations and events: y
     Log CTA/PSA/TTI Transactions: y
```

Table 30: Logging Levels form, page 2 of 2 fields, values, and description

Field	Values	Description
Log All Submission Failures ⚠ **SECURITY ALERT:** Form submission failures due to a security violation are always logged and are not affected by this field.	**y**(es)	When Communication Manager rejects a form submission for any reason (for example, an invalid entry in a field or a missing value), the event is logged.
	n(o)	When Communication Manager rejects a form submission for any reason, the event is not logged.
Log PMS/AD Transactions	**y**(es)	Property Management System (PMS) and Abbreviated Dialing (AD) events are logged.
	n(o)	Property Management System (PMS) and Abbreviated Dialing (AD) events are not logged.
Log IP registrations and events	**y**(es)	IP registrations and IP events are logged
	n(o)	IP registrations and IP events are not logged
Log CTA/TTI/PSA Transactions	**y**(es)	Customer Telephone Activation (CTA), Terminal Translation Initialization (TTI), and Personal Station Access (PSA) events are logged.
	n(o)	Customer Telephone Activation (CTA), Terminal Translation Initialization (TTI), and Personal Station Access (PSA) events are not logged.

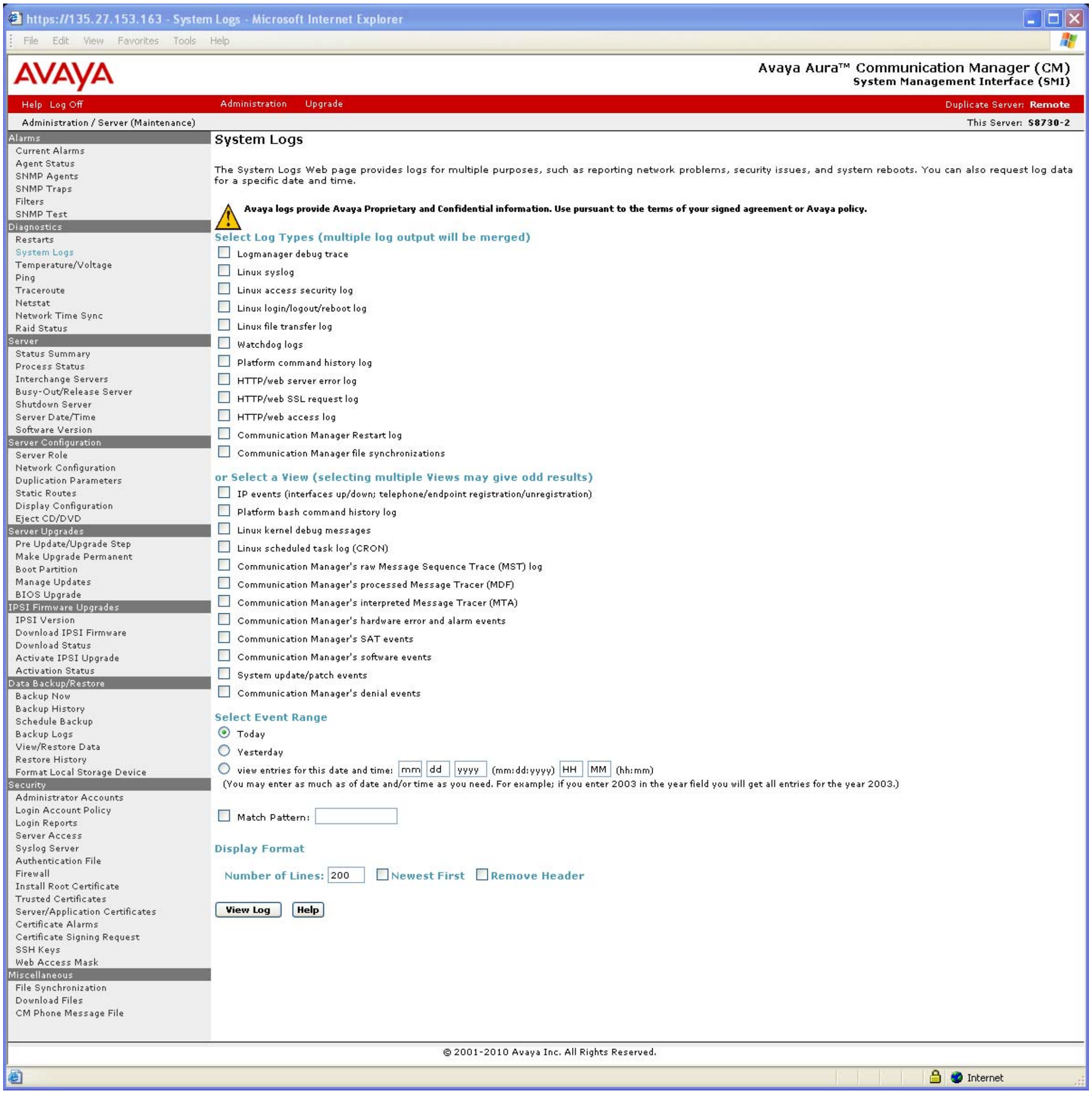
Accessing system logs through the Web

The Communication Manager System Management Interface (**Diagnostics** on the left-side navigation pane) displays the **System Logs** page (Figure 17). Some of the logs listed are part of the Linux syslog, while others are created by Communication Manager.

This form allows you to:

- Select multiple log types and merge data into a single view
- Select multiple views
- Select a range of time-specific events
- Search logs for a text string

Figure 17: System Logs page



System Logs

The System Logs Web page provides logs for multiple purposes, such as reporting network problems, security issues, and system reboots. You can also request log data for a specific date and time.

Avaya logs provide Avaya Proprietary and Confidential information. Use pursuant to the terms of your signed agreement or Avaya policy.

Select Log Types (multiple log output will be merged)

- □ Logmanager debug trace
- □ Linux syslog
- □ Linux access security log
- □ Linux login/logout/reboot log
- □ Linux file transfer log
- □ Watchdog logs
- □ Platform command history log
- □ HTTP/web server error log
- □ HTTP/web SSL request log
- □ HTTP/web access log
- □ Communication Manager Restart log
- □ Communication Manager file synchronizations

or Select a View (selecting multiple Views may give odd results)

- □ IP events (interfaces up/down; telephone/endpoint registration/unregistration)
- □ Platform bash command history log
- □ Linux kernel debug messages
- □ Linux scheduled task log (CRON)
- □ Communication Manager's raw Message Sequence Trace (MST) log
- □ Communication Manager's processed Message Tracer (MDF)
- □ Communication Manager's interpreted Message Tracer (MTA)
- □ Communication Manager's hardware error and alarm events
- □ Communication Manager's SAT events
- □ Communication Manager's software events
- □ System update/patch events
- □ Communication Manager's denial events

Select Event Range

- ● Today
- ○ Yesterday
- ○ view entries for this date and time: mm dd yyyy (mm:dd:yyyy) HH MM (hh:mm)

(You may enter as much as of date and/or time as you need. For example; if you enter 2003 in the year field you will get all entries for the year 2003.)

□ Match Pattern:

Display Format

Number of Lines: 200 □ Newest First □ Remove Header

© 2001-2010 Avaya Inc. All Rights Reserved.

More information

- Restricting web access to system logs on page 169
- Reading and interpreting the security logs on page 170

Chapter 4:   Network Security Integration

Firewall/topology configurations

Administering firewall settings in Communication Manager

Communication Manager firewall settings are administered through the Maintenance Web Page's Firewall page, which is a front-end to the standard Linux command **iptables**. IP Tables 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.

⚠ **WARNING:**
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, as it may adversely affect your Avaya media server.

Default Communication Manager firewall settings

Table 31: Default Communication Manager firewall settings on page 134 lists the Communication Manager firewall default settings:

Table 31: Default Communication Manager firewall settings

Input to server	Output from server	Service	Port/protocol
X	X	ftp	21/tcp
X	X	ssh	22/tcp
X	X	telnet	23/tcp
	X	domain	53/udp
		bootps	67/udp
		bootpc	68/udp
		tftp	69/udp
X	X	http	80/tcp
X	X	ntp	123/udp
X	X	snmp	161/udp
X	X	snmptrap	162/udp
X	X	https	443/tcp
	X	syslog	514/udp
		ldap	389/tcp
		ldaps	636/tcp
		radius	1812/udp
		securID	5500/udp
		safeword	5030/tcp
		http-ipphone	81/tcp
		https-ipphone	411/tcp
X		hp-sshd	2222/tcp
			1 of 3

Table 31: Default Communication Manager firewall settings

Input to server	Output from server	Service	Port/protocol
X	X	secure-sat	5022/tcp
X	X	def-sat	5023/tcp
X	X	echo-request	8/icmp
		ipsi-cmds	1956/tcp
		pcd-ipsi	5010/tcp
		ipsivsn	5011/tcp
		ipsilic	5012/tcp
		licsvr	5423/tcp
X	X	ewl	5424/tcp
		filesync-old	21873/tcp
X	X	filesync	21874/tcp
		vphone	1037/tcp
X		encrypted-h248	1039/tcp
X	X	h323gatestat	1719/udp
X	X	h323hostcall	1720/tcp
X		h248message	2945/tcp
X	X	sip	5060/tcp
X	X	sip-tls	5061/tcp
X		AEservices	8765/tcp
X		ip-signaling-1	5000:5021/tcp
X		ipsignaling-2	5024:9999/tcp
X		H.245	59000:59200/tcp
	X	gateway-compatibility	1024:65535/tcp
		arbiter	1332/udp
		arbiter	1333/udp
			2 of 3

Table 31: Default Communication Manager firewall settings

Input to server	Output from server	Service	Port/protocol
		dupmgr-swdup	5098/tcp
		dupmgr	12080/tcp
			3 of 3

Network "best practices"

- Separation of network functionality on page 136
- Layer 2 and Layer 3 hardening on page 137
- Designing VLAN groups for functional network segmentation on page 146
- How ARP spoofing facilitates network attacks on page 148
- Security strategies to combat ARP spoofing on page 148
- Security vulnerabilities with name and address management on page 149
- How Communication Manager addresses NIST recommendations on page 151
- Recommendations for preventing DoS attacks on page 156

Separation of network functionality

Control and bearer signaling separation

Communication Manager networks always have a control network and a bearer network. The control network carries call processing signals between the server, the gateways that connect endpoints, and the endpoints themselves. The bearer network carries the voice signals between endpoints. In some cases, as with the S8300 Server and with the Processor Ethernet link with an S8400 or S8500 Server, the control and bearer networks are carried over the same routes. In the case of an S8400, S8500, or S8700-Series Server that connect to the G650 Media Gateway, the control network is inherently separated because the server is connected to the IPSI TN2312BP circuit pack, which then carries control signaling to the gateways. The bearer network bypasses the server and the Media Processor circuit pack in the G650 Media Gateway connects the endpoints over the LAN.

The routes that control signals take between endpoints and the server can be different than the routes that bearer signals take. For example, when the Inter-Gateway Alternate Routing (IAGR) feature is enabled, control signals may continue to pass over the normal network of Ethernet switches, routers, C-LAN circuit packs, and IPSIs, the bearer signals might be routed over the Public Switched Telephone Network (PSTN) when the internal LAN/WAN network is overloaded. In the case of Avaya Softphone in telecommuter mode, IP signals related to a call are routed over an Internet Service Provider using a VPN to the user's P.C., and the bearer signaling is routed over the PSTN to the user's telephone.

Control and bearer signaling in VLANs

To add greater security, the control network and bearer network can be assigned to different VLANs. At some, or all, points in the route, the devices in the control network and bearer network might be the same. For example, since an IP telephone connects to a single port in an Ethernet switch, both the control and bearer signals are carried over that port connection. In this case, the IP telephone and Ethernet port must be assigned to both the control network and bearer network VLANs. Likewise, when using Processor Ethernet for gateway connections on the Communication Manager Server, the server must be assigned to both VLANs.

However, Ethernet switch and router, ports can be assigned to a single VLAN, thereby providing separate routes between endpoints. In this way, the VLANs are separated, thereby enhancing the security on both network segments.

Layer 2 and Layer 3 hardening

To ensure the Communication Manager system is secure, it is recommended that the customer harden, or secure, devices in the communication system's network at Layer 2, the data link layer, and Layer 3, the network layer, as defined by the Open Systems Interconnect (OSI) 7-layer network model. Communication Manager offers logging capabilities (see Configuring SNMP and syslog on page 116), which the customer can use to detect actual and potential security breaches. Additional host intrusion and network intrusion detection systems can also be added to the customer's network to detect security breaches at Layers 2 and 3.

The customer can also use a number of security features in other devices in the network to harden Layers 2 and 3 of the network. These devices include the G250-series, G350 Media Gateways, G430/G450 Media gateways, the IG550 Integrated Gateway, and third-party Ethernet switches and routers that provide LAN/WAN connectivity. If the Communication Manager server is an S8300 Server embedded in a G250-series, G350 Media Gateways or G430/G450 Media Gateways, the router capabilities of these gateways can protect data to Communication Manager without the need for a separate router.

The security features you can use are as follows:

- GRE tunneling
- IPSec VPN
- Access control lists

- 802.1X and LLDP

Note:
G450/G430 Media gateways do not support 802.1X and LLDP feature.

GRE tunneling

Generic Routing Encapsulation (GRE) is a multi-carrier protocol that encapsulates packets with an IP header and enables them to pass through the Internet through a GRE tunnel. A GRE tunnel is a virtual interface in which two routers serve as endpoints. The first router encapsulates the packet and sends it over the Internet to a router at the far end of the GRE tunnel. The second router removes the encapsulation and sends the packet towards its destination.

GRE tunneling does not encrypt data, and therefore, is not as secure as the IPSec protocol. However, GRE tunneling is easier to configure.

For more information on administering GRE tunneling on the G250-series or G350 Media Gateway, see *Administration for the Avaya G250 and G350 Media Gateways*, 03-300436. For more information on administering GRE tunneling on the G430 Media Gateway, see *Administration for the Avaya G430 Media Gateway, 03-603228.* For more information on administering GRE tunneling on the G450 Media Gateway, see *Administration for the Avaya G450 Media Gateway, 03-602055.* This document is available at http://support.avaya.com. For information on administering GRE tunneling on the IG550 Integrated Gateway, see the *J-series Services Router Administration Guide*. This document is available at http://www.juniper.net.

IPSec VPN

To harden Layers 2 and 3 in the communications network, the customer can use the IP Security (IPSec) protocol to transmit encrypted data. The near end device encrypts and then sends data, and the far end device unencrypts the data. IPSec can also be used for authentication between communication devices. The use of IPSec with tunneling creates a virtual private network (VPN). On the G250-series and G350 Media Gateways, IPSec support can be administered for optimal Quality of Service.

IPSec support is available on the G250-series and G350 Media Gateways and the IG550 Integrated Gateway. IPSec is available on the Motorola CN620 Mobile Office Device.

The G250-series and G350 Media Gateways and the IG550 Integrated Gateway offer the following features of IPSec:

- Standards-based IPSec implementation [RFC 2401-RFC 2412]
- Standard encryption and authentication algorithms for IKE and ESP. These algorithms include DES, TDES, AES (128-bit), MD5-HMAC, SHA1-HMAC, and IKE DH groups 1 and 2.
- ESP for data protection and IKE for key exchange.
- Quick Mode key negotiation with Perfect Forward Secrecy (PFS)

- IKE peer authentication through a preshared secret.
- Up to 50 IPSec peers for mesh and hub-and-spoke IPSec topologies.
- IPSec protection that can be applied on any output port and on many ports concurrently, for maximum installation flexibility.
- Per-interface security policy with bypass capability.
- Smooth integration with the onboard GRE tunneling feature. This tight integration provides the ability to use GRE over IPSec in a manner that maintains QoS for the encapsulated traffic.
- Random preshared-key-generation service.
- Load Balancing Resiliency through core routing features, such as backup interface, GRE and so on.
- Support for dynamic local address, which can be acquired through DHCP/Ethernet or IPCP/PPPoE. This is achieved by initiating Aggressive Mode, and identifying the Gateway through an FQDN string rather then IP address.
- Remote peer failover support.
- NAT traversal support – standard and legacy methods.
- Optimized bandwidth consumption by IP compression support and transport mode ESP support (can help when using GRE over IPSec).
- Enhanced service assurance by employing continuous IKE and IPSec SA establishment.
- Support for a comprehensive proprietary monitoring MIB.

For Communication Manager in an S8400, S8500, or S8700-Series Server, an intervening Avaya security gateway or a third party router must be administered to provide IPSec VPN security. Non-Avaya equipment that is compatible with the Avaya media gateway functionality using IPSec include:

- Cisco IOS 3660 v12.3
- Cisco IOS 2600 v12.3 / v12.2
- Cisco PIX 525 Firewall v6.3(3)
- Checkpoint NG with application intelligence (R54) Build 289
- Juniper Netscreen NS-50 Gateway

For more information on IPSec support on the G250-series or G350 Media Gateway, see *Application Note: G350 and G250 R3.0 IPSec VPN*, which is available on the Avaya support Web site at:

http://support.avaya.com/elmodocs2/g350/AppNotes_G350_G250_R3_ndezent_070605.pdf

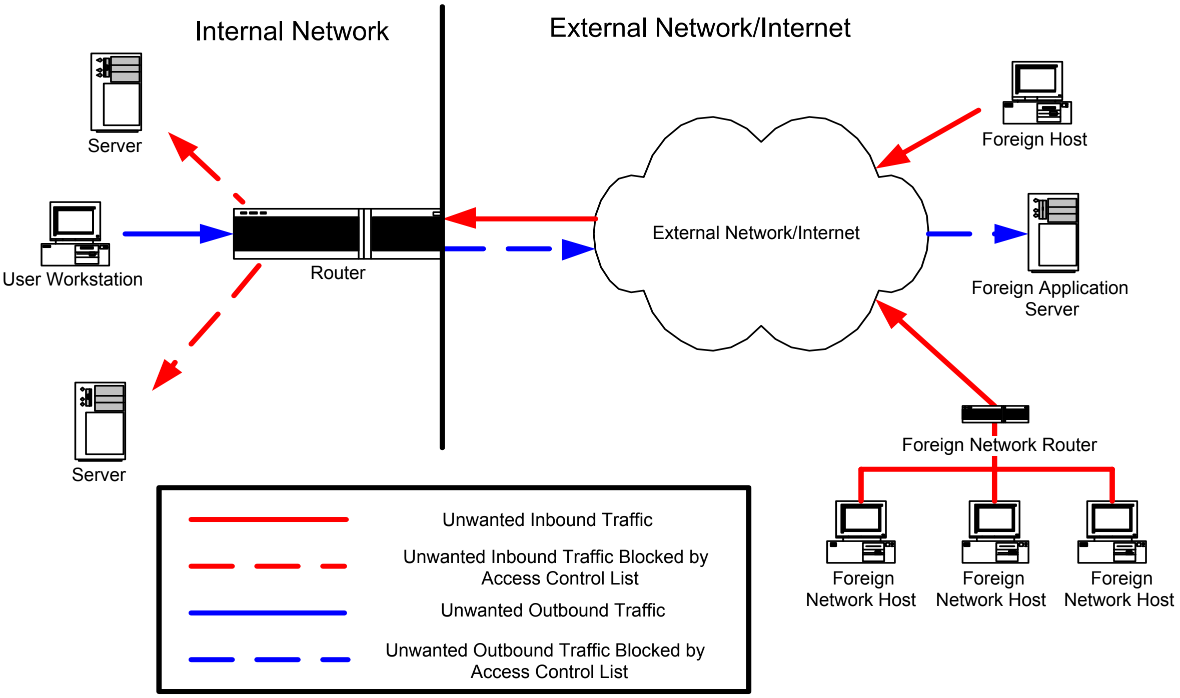
Also see *Administration for the Avaya G250 and G350 Media Gateways*, 03-300436. For information on administering IPSec on the IG550 Integrated Gateway, see the *J-series Services Router Administration Guide*.

Access control lists

On the Avaya G250, G350, G430, G450 Media Gateways and the IG550 Integrated Gateway, you can use access control lists (ACLs) to determine which applications, networks, and users can access hosts on your network. Also, you can restrict internal users from accessing specific sites or applications outside the network. Access control lists can be based on permitting or denying specific values or groups of IP addresses, protocols, ports, IP fragments, or DSCP values. Figure 18: Network Security using access control lists on page 140 illustrates how access control lists are used to control traffic into and out of your network.

Note:
The G700 Media Gateway does not provide ACL capabilities or DoS protection. A separate customer-provided router must provide these capabilities.

Figure 18: Network Security using access control lists


Internal Network
External Network/Internet
Server
User Workstation
Router
Server
External Network/Internet
Foreign Host
Foreign Application Server
Foreign Network Router
Foreign Network Host
Foreign Network Host
Foreign Network Host
Unwanted Inbound Traffic
Unwanted Inbound Traffic Blocked by Access Control List
Unwanted Outbound Traffic
Unwanted Outbound Traffic Blocked by Access Control List

Access control list rule specifications

You can use access control lists to control which packets are authorized to pass through an interface. When a packet matches a rule on the access control list, the rule specifies whether the media gateway:

- Accepts the packet or drops the packet
- Sends an ICMP error reply if it drops the packet

- Sends an SNMP trap if it drops the packet

For more information see,

Administration for Avaya G250 and the G350 Gateways (03-300436).

Administration for the Avaya G430 Media Gateway (03-603228).

Administration for the Avaya G450 Media Gateway (03-602055).

External authentication of server administrator accounts

Communication Manager 4.0 and later support standard Authentication, Authorization, and Auditing Services (AAA Services) for authenticating administrator logins. Customers who use a central server to store and maintain administrator account (login) information can add Avaya account information to the central authentication infrastructure, external to the Communication Manager server, already in place.

Avaya’s support of AAA Services allows, through an authentication server:

- Centralized control of enterprise logins and passwords
- Enforcement of password aging, minimum length, and reuse requirements
- Avaya product adherence to the enterprise corporate security standards regarding logins and passwords

See:

- External authentication accounts on page 142
- External authentication accounts on page 142
- External authentication servers on page 143

External authentication accounts

External authentication account server requirements are listed in Table 32: External Authentication Accounts.

Table 32: External Authentication Accounts

External authentication accounts	Required external servers	Authentication information
LDAP - based accounts	Require an LDAP server compatible with the LDAP client from www.openldap.org. LDAP servers tested with Communication Manager are: ● The server from www.openldap.org ● Microsoft Active Directory ● SunOne Directory Service	The LDAP module that resides on the Avaya Server authenticates with an external LDAP server. When logins are configured at OpenLDAP: ● Avaya Services logins are authenticated locally (Communication Manager) ● Customer logins are authenticated either locally or on the LDAP server
RADIUS - based accounts	Require: ● a RADIUS server compatible with the client from www.freeradius.org ● a parallel local host account or an LDAP account for authorization information	When logins are configured through Communication Manager/RADIUS: ● Avaya Services logins are authenticated locally (Communication Manager) ● Customer logins are authenticated at RADIUS and authorized locally (Communication Manager)
Token - based accounts ● RSA SecurID ● Secure Computing SafeWord	● RSA SecurID (provides only user authentication) or ● Secure Computing SafeWord (provides only user authentication) Require a parallel host account or an LDAP account for authorization information.	● Can be used directly from the Avaya Server, when a license is purchased from the vendor and software is installed on the Avaya Server. ● Can be used behind a RADIUS server.

External authentication servers

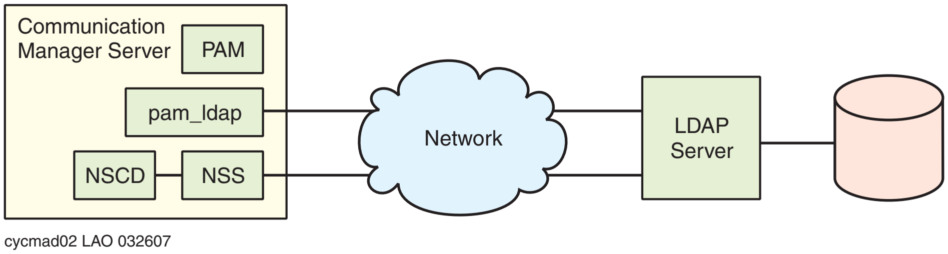
At a minimum, Avaya supports only customer-provided Open LDAP and RADIUS servers on Avaya servers, gateways, and any application that offers user or administrative access and authentication. Communication Manager also supports SafeWord and SecurID for external authentication. Avaya supports no other external identity management systems.

See the *Communication Manager Administrator Logins White Paper* on http://support.avaya.com/elmodocs2/white_papers/CM_Administrator_Logins.pdf for detailed information on configuring external AAA Servers.

LDAP servers

The tested configuration for external LDAP servers with Name Service Switch (NSS)/ Name Service Caching Daemon (NSCD) is shown in Figure 19. Login requires an entry in LDAP only.

Figure 19: LDAP server authentication configuration

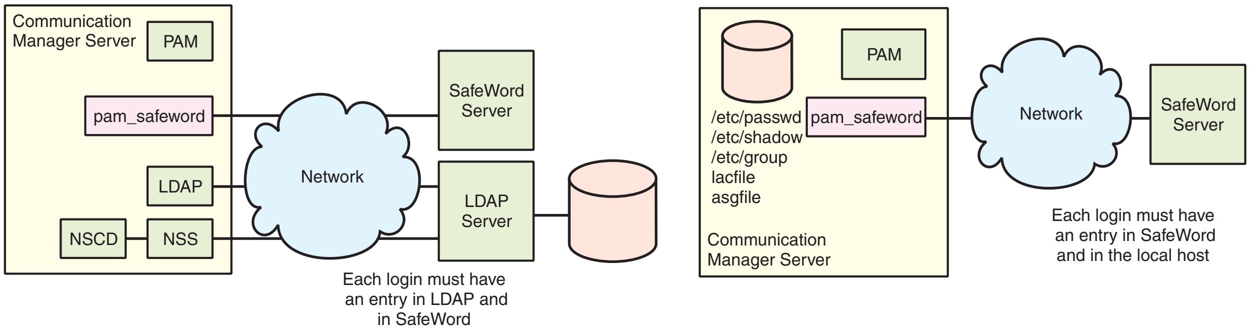


RADIUS servers

External RADIUS provides only user authentication and accounting as shown in Figure 20: RADIUS server authentication configurations on page 144.

Note:
Communication Manager Branch Gateways support only RADIUS servers.

Figure 20: RADIUS server authentication configurations

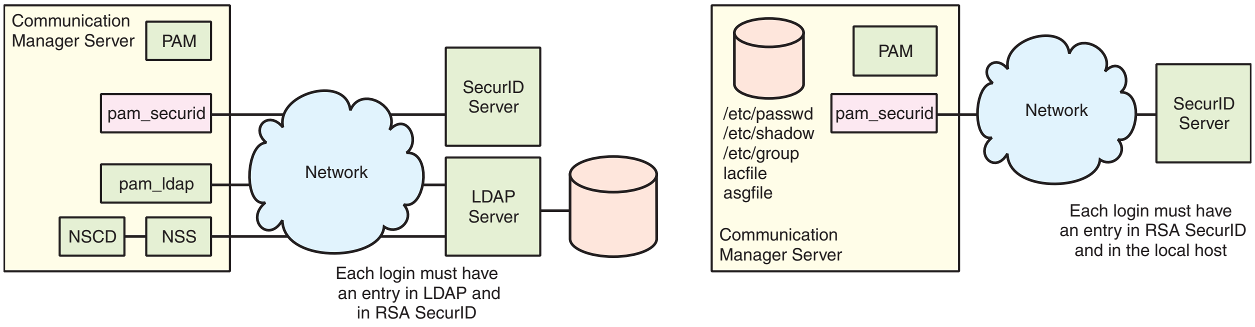

Communication Manager Server
PAM
pam_safeword
LDAP
NSCD
NSS
Network
SafeWord Server
LDAP Server
Each login must have an entry in LDAP and in SafeWord
/etc/passwd
/etc/shadow
/etc/group
lacfile
asgfile
PAM
pam_safeword
Communication Manager Server
Network
SafeWord Server
Each login must have an entry in SafeWord and in the local host

cycmad04 LAO 032607

Token servers

RSA SecurID is a token-based authentication method from RSA Security that provides only user authentication. Figure 21: RSA SecurID server authentication configurations shows configurations with an LDAP server and with a local host (no LDAP server).

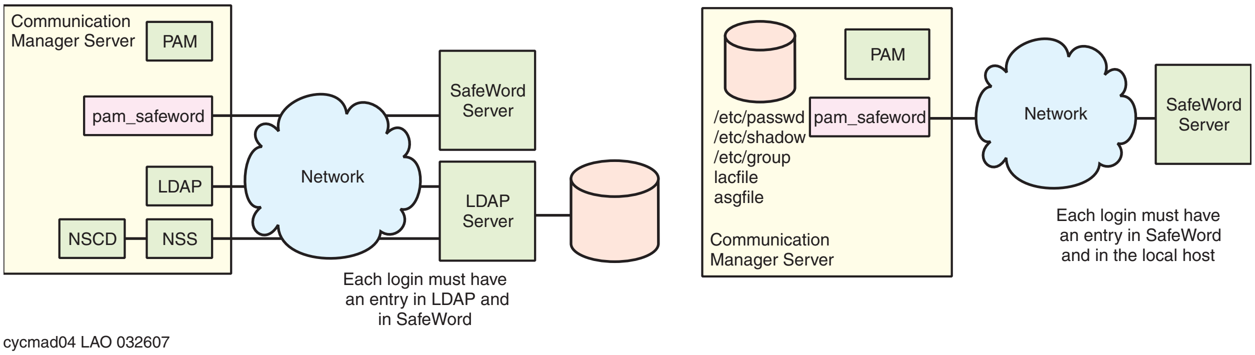
Figure 21: RSA SecurID server authentication configurations


Communication Manager Server
PAM
pam_securid
pam_ldap
NSCD
NSS
Network
SecurID Server
LDAP Server
Each login must have an entry in LDAP and in RSA SecurID
/etc/passwd
/etc/shadow
/etc/group
lacfile
asgfile
PAM
pam_securid
Communication Manager Server
Network
SecurID Server
Each login must have an entry in RSA SecurID and in the local host

cycmad03 LAO 032607

Secure Computing SafeWord is a token-based authentication method from RSA Security that provides only user authentication. Figure 22: SafeWord server authentication configurations shows configurations with an LDAP server and with a local host (no LDAP server).

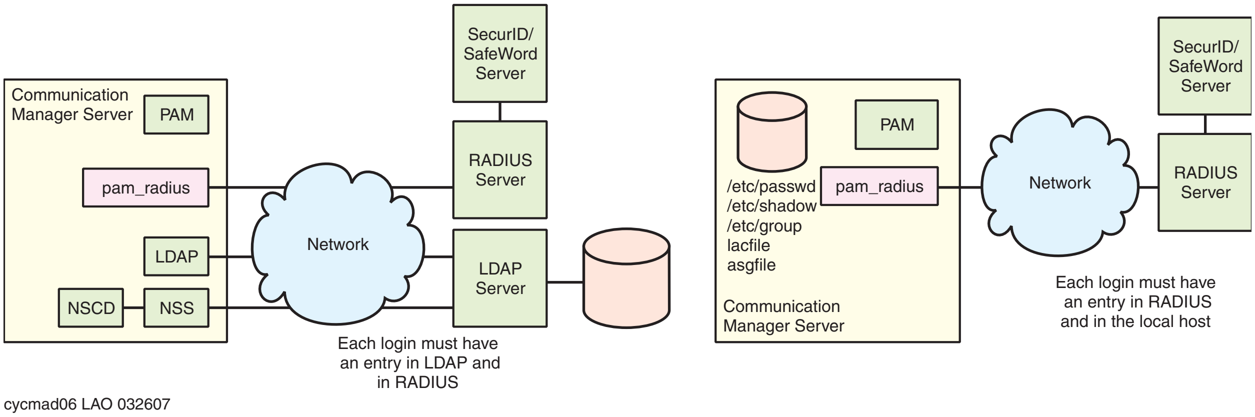
Figure 22: SafeWord server authentication configurations


Communication Manager Server
PAM
pam_safeword
LDAP
NSCD
NSS
Network
SafeWord Server
LDAP Server
Each login must have an entry in LDAP and in SafeWord
cycmad04 LAO 032607
/etc/passwd
/etc/shadow
/etc/group
lacfile
asgfile
PAM
pam_safeword
Communication Manager Server
Network
SafeWord Server
Each login must have an entry in SafeWord and in the local host

RADIUS plus token servers

Figure 23: Radius plus token authentication configurations shows an example of another authentication configuration: RSA SecurID and SafeWord used behind an external RADIUS server.

Figure 23: Radius plus token authentication configurations



Administering external authentication

The Communication Manager default configuration does not contain an entry for an external AAA server. All accounts are authenticated on the local host.

To activate use of an external AAA server, edit the `/etc/pam.d/mv-auth` file to incorporate the appropriate lines for the server being used. Edit additional configuration files corresponding to the needs of the AAA service. Customers, not Avaya Services, activate external AAA services. Customer provides and owns the AAA server on their network and they alone have the information necessary to set up clients on the Communication Manager servers.

Additional information

For information regarding configuring external AAA servers, see:

- *Communication Manager Administrator Logins* White Paper at http://support.avaya.com/elmodocs2/white_papers/CM_Administrator_Logins.pdf
- http://www.kernel.org/pub/linux/libs/pam

  This Web site contains PAM documentation such as the System Administrators’ Guide.

802.1X and LLDP

The 802.1x protocol provides an authentication of devices at Layer 2. LLDP is a protocol that enables devices to identify themselves to other devices in the network. Together, these protocols prevent unauthorized access to ports and devices at Layer 2.

Designing VLAN groups for functional network segmentation

The Communication Manager network and data networks should be logically separated using virtual LANs (VLANs). VLANs can be set up to isolate devices in the network from other devices, but also can be set up to allow communication between devices in different VLANs for only specifically-designated protocols.

For network separation to be effective, several different protected VLANs must be established. First, all network devices not specifically used to support telephony should be placed on data VLANs. Data VLANs support PCs, file servers, email servers, and domain controllers. Communication Manager network devices should be placed on different VLANs depending on their role in the network. Limiting each VLAN to like devices and protocols makes the development, implementation, and management of security features much easier. All standalone IP telephones should be placed in their own IP telephone VLAN(s). The Communication Manager server itself should be placed in a different VLAN, depending on the VoIP protocol the customer implements. A Communication Manager sever, which is an H.323 server, should be on an H.323-only VLAN. A SIP server, if any, should be placed on a SIP VLAN. Also, Softphones should also be placed on dedicated VLAN(s).

The telephony and data VLANs should have their own servers for standard network services such as DNS, DHCP, and NTP. This is necessary because traffic from these services should not have to cross the perimeter between the telephony network and data VLANs.

To prevent an attacker who has physical access to the network from bypassing any VLAN separation by simply unplugging the IP phone's network cable and attaching an attack computer, switch port level security must also be implemented. The customer should implement 802.1x authentication on any IP telephones, Ethernet switches, G250 or G350 Media Gateways, or IG550 Integrated Gateways.

The Communication Manager server VLAN typically should contain the Communication Manager server and other authentication and authorization devices such as the Radius server, a DHCP server, a DNS server, and an NTP server. The IP telephone VLAN contains IP phones, IP interfaces to the IP telephones, the access controller gateway, and the connecting media gateway. The gateway VLAN would normally contain gateways to external network such as the PSTN. However, since the media gateways typically connect to both lines and trunks, the line ports can be assigned to the IP telephone VLAN and the trunks can be assigned to a separate trunk VLAN.

Traffic filtering and firewalling

Dividing the network into multiple VLANs does not provide any benefit if the traffic between the VLANs is not restricted. However, the Communication Manager VLAN must communicate with the IP telephone and media gateway VLANs using signaling protocols to setup and authorize calls. The IP telephone VLANs must exchange media traffic with the gateway VLANs and with the server VLAN if voicemail applications run on the servers. The Communication Manager Server and phone VLANs also share administrative protocols so that the Communication Manager Server can configure IP telephones. These may be different protocols than those used by the administrative VLAN. And the Communication Manager Server VLAN might provide network services, such as NTP, which might be used by most devices on the Communication Manager network.

Traffic between IP telephony VLANs must be controlled by packet filtering routers or Layer 3 switches. The access control lists (ACLs) on these devices must be configured to only allow IP phones to connect to the Communication Manager Server the phone needs to function and vise versa. In many cases, this means that only VoIP signaling protocols need to be allowed between telephones and the Communication Manager server. Filtering should be done based on IP address, port number, and TCP/IP flags, not port number alone.

The Communication Manager and data VLANs are usually separated by stateful Layer 3 & 4 traffic filtering configured to block most protocols but to allow passage of those protocols required for IP telephony features.

As much as possible, traffic between the Communication Manager Server and the data network should be minimized. For example, the customer should disable the Web interface on the IP telephones, and allow users to manage the phone on a central server that would securely push changes to the phone. To further manage traffic between the Communication Manager VLANs and the data VLANs, the customer can use the Communication Manager Firewall to eliminate some types of traffic between the Communication Manager network VLANs and the data VLANs. However, router firewalls might be used to provide more extensive firewall protection between VLANs.

Assigning VLANs in Communication Manager

Communication Manager software allows the customer to assign VLANs to IP interfaces such as the C-LAN or media processor circuit packs and to IP telephones. In these cases, the VLAN is automatically separate from any normal data-only VLANs.

Assigning VLANs in the G250-series, G350, G430 and G450 Media Gateways

The customer can assign the ports on the G250-series, G350, G430, G450 Media Gateways in a variety of ways:

- Assign a port to one or more specific VLANs
- Assign a port to support all VLANs known to the media gateway

The customer can also assign a VLAN to the S8300 Server, if installed on the media gateway.

How ARP spoofing facilitates network attacks

A server, gateway, or IP telephone needs the Media Access Control (MAC) address of the target networked device in order to communicate with that device. And vice-versa, any device that tries to communicate with an Avaya server, gateway, or IP telephone needs the MAC address of the server/gateway/IP telephone. When the MAC address is not yet known, an Address Resolution Protocol (ARP) request is sent to a known IP address to determine what the MAC address is. For example, Device A initiates communication with Device B by sending an Address Resolution Protocol (ARP) request along with the IP address of device B. Device B then replies to device A and sends device B’s MAC address. Device A then updates its ARP cache to save the MAC address for any future communications with the device B.

An attacker uses an ARP spoofing tool to identify the IP and MAC addresses of the device (server, gateway, or IP telephone) to be attacked. Since the initiating device sends an ARP request as a broadcast, the attacker’s ARP- spoofing tool can listen for these requests. Once the spoofing tool has an IP address for Device A and Device B, it can send fake ARP replies to each device. Each device then changes the ARP cache for that device such that Device A has the MAC address of the attacker’s host instead of Device B’s MAC address, and Device B has the MAC address of the attacker’s host instead of Device A’s MAC address. This impersonation causes IP traffic between the target devices and other locales to be routed through the attacker’s host. With sniffing tools, the attacker can then eavesdrop on calls and sniff the packets for other data such as user names, logins, and passwords. This rerouting and manipulations of data is called a "man-in-the-middle" attack.

Security strategies to combat ARP spoofing

There is no universal defense against ARP spoofing. One possible defense is the use of static (non-changing) ARP entries. Since static entries cannot be updated, spoofed ARP replies are ignored. To prevent spoofing, the ARP tables would have to have a static entry for each machine on the network. The overhead in deploying these tables, as well as keeping them up to date, is not practical for most LANs, including those that incorporate Communication Manager systems.

Avaya recommends the following practical defenses:

- Dividing the network into separate domains or subnets.

  ARP spoofing cannot occur when the communicating devices are in different subnets. Media gateways and the IP telephones associated with those gateways can be administered in separate domains as much as is practical to provide some deterrence to ARP spoofing.

Security vulnerabilities with name and address management

Domain Name System (DNS) servers and Dynamic Host Configuration Control (DHCP) servers, as with other network devices, are susceptible to ARP-spoofing and "man-in-the-middle" attacks. Because these types of servers are repositories of information for multiple devices on a customer's network, the need for security of these servers is even greater than the security needs of end-point devices.

A DNS server associates host names and IP addresses so that names can be used to access devices on the network.

DHCP is a protocol used by networked servers, gateways, and IP telephones to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server. The DHCP server also ensures that all IP addresses are unique. Thus, IP address pool management is performed by the DHCP server, not by a human network administrator.

DHCP vulnerabilities

Each IP phone automatically sends out a DHCP request for an IP address with which to register. The DHCP server then sends the IP phone the IP address of the Communication Manager server and any TFTP servers and LSPs that are know to the DHCP server. The IP phone then registers automatically with Communication Manager.

This sequence could open the server, as well as any IP telephones, to attack if the attacker can successfully spoof the DHCP server. DHCP has an inherent vulnerability in that it is not an authenticated protocol and thus it is open to spoofing. An attacker can provide incorrect network settings to a phone, which could result in a denial of service, redirection of calls to malicious servers, or man-in-the-middle attacks. Malicious DHCP clients can also cause a denial of service by continuously requesting IP addresses until none are left for legitimate devices.

Also, an IP telephone's firmware or configuration file could be modified in one of two ways. First, once the DHCP server has been spoofed, an attacker could perform a man-in-the-middle attack to intercept and replace the files as they are downloaded from the server. Second, an attacker could compromise the server storing the firmware and configuration files. This is a more serious problem because control of a download server enables an attacker to easily attack all phones in an organization.

DHCP security

To create greater security in a network that uses DHCP servers, you use one or more of the following security measures.

- Assign static IP addresses to the Communication Manager server and media gateways. See the appropriate installation document for Communication Manager servers (S8300, S8400, S8500-series, S8700-series).

  You can also assign static IP addresses to IP telephones that serve critical functions. However, this option is often impractical when the system's IP telephones are both numerous and frequently changing. In addition, with a static IP address, each time an IP telephone reboots, the telephone does not automatically reregister with its servers. See *4600 Series IP Telephone LAN Administrator Guide,* 555-233-507.

  As with the Communication Manager server, C-LAN and media processor circuit packs are assigned static IP addresses. See *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504.

- Limit the use of automatic registration and DHCP to periods of significant IP phone deployment and disable DHCP once registration is complete. DHCP can also be more safely enabled when protected by anti-spoofing features that keep associations of IP address, MAC address, and switch port in access and infrastructure devices.

  Because a loss of LAN connectivity causes each IP telephone to search for an IP address, disabling DHCP might be impractical. In the event of a break in LAN connectivity, IP telephones cannot reregister until the DHCP server is enabled again. Waiting for the DHCP server to be re-enabled could cause a significant length of time without IP telephone support.

- Use separate DHCP servers to support the devices in the IP telephony VLAN or VLANs and the devices in the rest of the data network. Since ARP-spoofing cannot work across VLAN boundaries, attacks on DHCP servers are limited to the data network only or the VoIP network only. In addition, if VLANs are associated with a geographical location only, attacks on a particular DHCP server are limited to physical access points within that location.

  Use the Communication Manager IP Interface screen and the Network Mapping screen to assign VLANs to IP telephones and media gateways. In addition, use the Locations, Location Parameters, and Network Region screens to further define the characteristics of each VLAN. And finally, administer a DHCP server support each VLAN.

- Configure access control lists on routers and firewalls to limit access to the DHCP client ports.

- Enable link layer authentication (such as 802.1x) on IP telephones and media gateways before connecting to the network.
- Administer network switches, when possible, to associate Ethernet address, IP address, and switch port. When a packet is received on a port with an address that does not match, it is dropped.
- Encrypt all firmware and configuration files that must be downloaded over the network. Require that each phone has the signature verification key loaded on the phone in a secure manner such as on an isolated network or over a direct serial connection. The phone must verify the signature on every file it downloads from the network and reject any files with invalid signatures. The signing key must be saved in a secure place and not be stored on the download server.

  IP telephones support HTTPS for downloading firmware. In addition, SIP telephones support signed file downloads.

  Media gateways support only SCP for download/upload.
- Provide firmware and configuration files from a server using SCP or HTTPS only and require authentication.

DNS vulnerabilities

Like DHCP, DNS servers are vulnerable to spoofing. Not only can the IP address associated with names be spoofed, but the names themselves can be spoofed with names of similar-looking spellings. Such vulnerabilities can lead to "man-in-the-middle" attacks across many devices in the network.

DNS security

To create greater security in a network that uses DNS servers, use one or more of the following security measures:

- Use separate DNS servers to support the devices in the IP telephony VLAN or VLANs and the devices in the rest of the data network.
- Enable DNSSec encryption on all DNS servers and enable DNS resolvers with DNSSec support on all DNS clients in the network. This solution, however, means that the DNS server or servers transmit the entire list of names within a DNS zone when it queries or responds to DNS requests. Such a transmission may be unlawful in some countries and could enable an attacker to determine the existence of the DNS clients in the zone.

How Communication Manager addresses NIST recommendations

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) has identified a number of security risks associated with VoIP communications systems and recommend methods for reducing those risks. The risks fall under the following categories:

- Confidentiality and privacy
- Integrity issues
- Availability and Denial of Service

Confidentiality and privacy

In a telecommunications switch, eavesdropping on conversations is an obvious concern, but the confidentiality of other information on the switch must be protected to defend against toll fraud, voice and data interception, and denial of service attacks. When compared to TDM systems, VoIP communications system offer increased opportunities for eavesdroppers because of the many nodes in a packet network that may be accessed surreptitiously.

The following vulnerabilities to confidentiality and privacy are described below, each with a NIST recommendations for reducing those vulnerabilities and a description of how Communication Manager addresses the vulnerability:

- Switch default password vulnerability on page 152
- Classical wiretap vulnerability on page 153
- ARP cache poisoning and ARP floods on page 153
- Web server interfaces on page 153
- IP phone subnet mask vulnerability on page 153
- Extension to IP address mapping vulnerability on page 154

Switch default password vulnerability

NIST recommendation: Default administrative or root passwords should be changed to prevent wiretapping of conversations on the network with port mirroring or bridging. If possible, remote access to the graphical user interface should be disabled to prevent the interception of plaintext administration sessions. When possible, a direct USB connection to the administrative interface is recommended. Also, consider disabling port mirroring on the switch.

How Communication Manager addresses the vulnerability: Communication Manager default passwords are automatically changed when the Communication Manager server is installed. A super-user login must be administered before the installation can be completed.

You cannot disable the Graphical User Interface (GUI) on Communication Manager because key functions are available only through the GUI.

Classical wiretap vulnerability

Attaching a packet capture tool or protocol analyzer to the VoIP network segment enables easy interception of voice traffic.

NIST recommendation: Establish good physical security policy for the deployment environment to prevent attachment of a packet capture tool or protocol analyzer to the VoIP network segment. Disable the hubs on IP Phones and use an alarm system for notifying the administrator when an IP telephone has been disconnected so that the system will not be open to this kind of attack.

How Communication Manager addresses the vulnerability: Avaya's IP telephones have the option of manually disabling the secondary hub. Communication Manager logs events such as the disconnect of an IP telephone are reported to Communication Manager. In addition, an alarm is generated when an IP telephone is disconnected. See *Maintenance Commands for Avaya Servers, and Media Gateway*s, 03-300430

ARP cache poisoning and ARP floods

An ARP flood attack, in which overwhelming number of ARP requests are sent, could result in broadcast ARP responses, which in turn could render the network vulnerable to conversation eavesdropping. Corruption of the ARP cache could result in traffic rerouting to intercept voice and data traffic.

NIST recommendation: Use authentication mechanisms provided wherever possible and limit physical access to the VoIP network segment.

How Communication Manager addresses the vulnerability: See Security strategies to combat ARP spoofing on page 148.

Web server interfaces

When a web server interface is used for remote or local administration, an attacker with access to the local network may be able to sniff plaintext HTTP packets to gain confidential information.

NIST Recommendation: If possible, do not use an HTTP server. If it is necessary to use a web server for remote administration, use the more secure HTTPS (HTTP over SSL or TLS) protocol.

How Communication Manager addresses the vulnerability: Communication Manager supports HTTPS over SSL and TLS.

IP phone subnet mask vulnerability

An attacker can assign a subnet mask and router address to an IP telephone, which can cause most or all of the packets the telephone transmits to be sent to an attacker's MAC address. This kind of intrusion is all but undetectable.

NIST recommendation: A firewall filtering mechanism can reduce the probability of this attack. Remote access to IP telephones is a severe risk.

How Communication Manager addresses the vulnerability: Communication Manager has its own firewall, which allows the customer to turn on or turn off various protocols and ports when not needed. In addition, the G250-series and G350 Media Gateways and the IG550 Integrated Gateway support access control lists for traffic accessing the Communication Manager network.

Extension to IP address mapping vulnerability

Discovering the IP address corresponding to any extension requires only calling that extension and getting an answer. A protocol analyzer or packet capture tool attached to the hub on the dialing instrument can see packets directly from the target instrument once the call is answered. Knowing the IP address of a particular extension is not a compromise in itself, but makes it easier to accomplish other attacks. For example, if the attacker is able to sniff packets on the local network used by the switch, it is easy to pick out packets sent and received by a target phone. Without knowledge of the IP address of the target phone, the attacker's job may be much more difficult to accomplish and require much longer, possibly resulting in the attack being discovered.

NIST recommendation: Disable the hub on the IP telephone to prevent this kind of attack. When necessary, it is a simple task to turn the hub back on.

How Communication Manager addresses the vulnerability: Avaya's IP telephones have the option of manually disabling the secondary hub. See Secure updates of Avaya software and firmware on page 205.

Integrity issues

Integrity of information means that information remains unaltered by unauthorized users. Misuse may involve legitimate users (that is, insiders performing unauthorized operations) or intruders. A legitimate user may perform an incorrect, or unauthorized operational function because of several factors, including the possibility that the level of access permission granted to the user is higher than what the user needs. An attacker might be able to alter data because:

- An intruder masquerades as a legitimate user and accesses an operations port of the switch. Then, the intruder can perform such operations as:
  - ï Disclosing confidential data
  - ï Causing service deterioration by modifying the system software
  - ï Crashing the system
  - ï Removing all traces of the intrusion (for example, modifying the security log)
- At certain times the system becomes vulnerable because it is not in a secure state. For example:

- ï After a system restart or during a disaster recovery, the old security features may have been reset to insecure settings, and new features might not yet be activated. (For example, all old passwords might have reverted to the default system-password, even though new passwords are not yet assigned.)
- ï At the time of installation the switch may be vulnerable until the default security features have been replaced.

DHCP server insertion attack

When an IP telephone requests a response from a DHCP server, a rogue DHCP server can initiate a response with data fields containing false information. This attack allows for possible "man in the middle" attacks on the media gateway and supported IP telephones. Also, many methods exist with the potential to reboot an IP telephone remotely, for example, ping flooding and MAC spoofing, which artificially generate DHCP server requests.

NIST recommendation: If possible, use static IP addresses for the IP Phones. This use removes the necessity of using a DHCP server. Further, using a state-based intrusion detection system can filter out DHCP server packets from IP telephone ports, allowing this traffic only from the legitimate server.

How Communication Manager addresses the vulnerability: With Communication Manager, a number of measures are available to help minimize the risk of DHCP server insertion. See DHCP security on page 150.

TFTP server insertion attack

When an IP telephone is resetting, a rogue TFTP server might respond to a TFTP request before the legitimate TFTP server. Then the attacker might reconfigure the target phone.

NIST recommendation: Use a state-based intrusion detection system to filter out DHCP server packets from IP telephone ports, allowing such traffic only from the legitimate server. Also, use IP telephones that can download signed binary files.

How Communication Manager addresses the vulnerability: Communication Manager and Avaya's IP telephones support secure file transfer using HTTPS protocols. The G250-series and G350, G430, G450, Media Gateways and the IG550 Integrated Gateway support SCP protocol for configuration files transfer. See Secure backups of Communication Manager data and translations on page 204.

Availability and Denial of Service

Availability refers to the notion that information and services be available for use when needed. Attacks exploiting vulnerabilities in the system software or protocols may lead to deterioration or even denial of service. Any network may be vulnerable to denial of service attacks, simply by overloading the capacity of the system. With VoIP the problem may be especially severe, because of its sensitivity to packet loss or delay.

CPU resource consumption attack without any account information

An attacker with remote terminal access to the server can force a system restart (shutdown all/ restart all) by providing the maximum number of characters for the login and password buffers multiple times in succession. Additionally, IP telephones can reboot as a result of this attack. In addition to producing a system outage, the restart might not restore uncommitted changes or, in some cases, might restore default passwords, which would introduce intrusion vulnerabilities.

NIST recommendation: The deployment of a firewall disallowing connections from unnecessary or unknown network entities is the first step to overcoming this problem. However, there is still the opportunity for an attacker to spoof a MAC and IP address, circumventing the firewall protection.

How Communication Manager addresses the vulnerability: Communication Manager has its own firewall, which allows the customer to turn on or turn off various protocols and ports when not needed. In addition, the G250-series, G350, G430, G450 Media Gateways and the IG550 Integrated Gateway support access control lists for traffic accessing the Communication Manager network. Finally, you can use anti-ARP spoofing strategies in case of an attacker who bypasses the firewall with ARP spoofing. See Security strategies to combat ARP spoofing on page 148.

Default password vulnerability

See Switch default password vulnerability on page 152.

Account lockout vulnerability

An attacker might provide several incorrect login attempts at the telnet prompt until the account becomes locked out.

The account is unable to connect to the machine for the set lockout time.

NIST recommendation: If remote access is not available, this problem can be solved with physical access control.

How Communication Manager addresses the vulnerability: On Communication Manager systems, Telnet is disabled by default. SSH is the recommended protocol for remote access. In addition, physical access through a serial console is available on every Communication Manager server.

Recommendations for preventing DoS attacks

To help mitigate DoS attacks Avaya recommends specific Communication Manager administration for:

- Mitigating call processing overloads

- Remote Managed Services
- Signaling groups

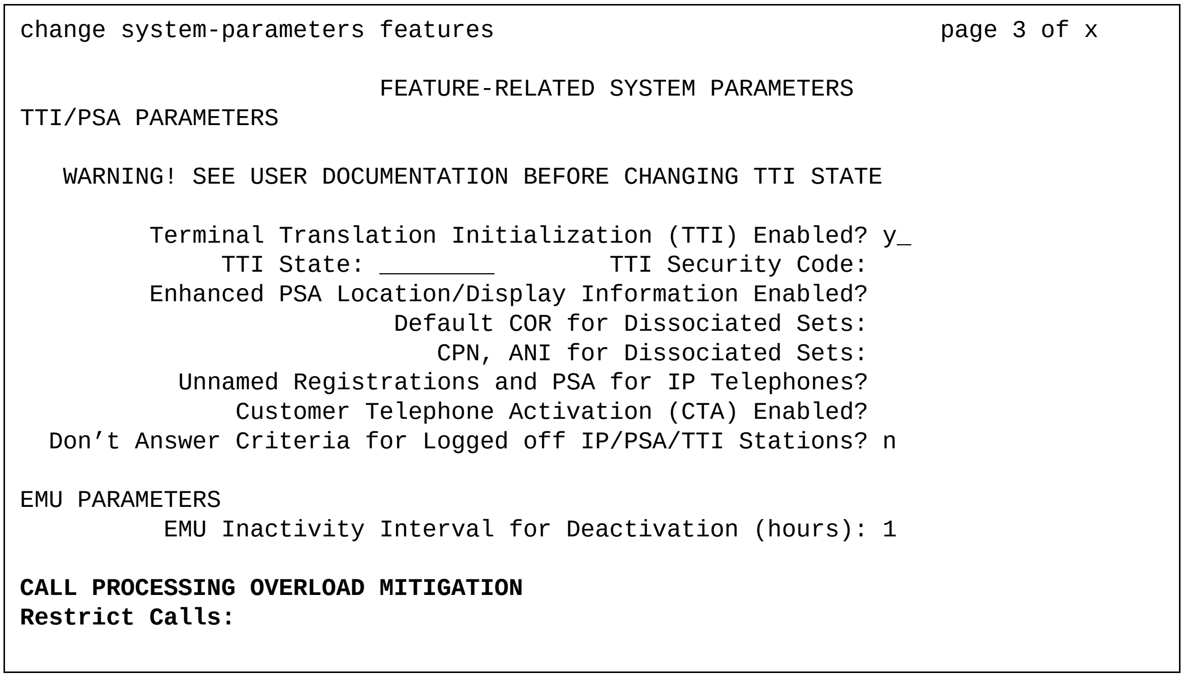
Mitigating call processing overloads

Communication Manager monitors and reacts to call processing overload conditions as a defense against DoS attacks. Administration allows customized, adaptive traffic shaping to throttle in- and outbound trunk traffic.

Call processing overload threshold events (92.5% overload condition) are logged in the Communication Manager event log.

Administer call processing overload on the Communication Manager **Feature-Related System Parameters** form (**`change system-parameters`** ***`features`***).

Figure 24: Feature-Related System Parameters screen



```
change system-parameters features                                page 3 of x

                         FEATURE-RELATED SYSTEM PARAMETERS
TTI/PSA PARAMETERS

   WARNING! SEE USER DOCUMENTATION BEFORE CHANGING TTI STATE

         Terminal Translation Initialization (TTI) Enabled? y_
              TTI State: ________        TTI Security Code:
         Enhanced PSA Location/Display Information Enabled?
                          Default COR for Dissociated Sets:
                             CPN, ANI for Dissociated Sets:
           Unnamed Registrations and PSA for IP Telephones?
               Customer Telephone Activation (CTA) Enabled?
  Don’t Answer Criteria for Logged off IP/PSA/TTI Stations? n

EMU PARAMETERS
          EMU Inactivity Interval for Deactivation (hours): 1

CALL PROCESSING OVERLOAD MITIGATION
Restrict Calls:
```

Use the recommendations in Table 33: Field values and descriptions for Restrict Calls on page 158 to administer the **Restrict Calls** field on the **Feature-Related System Parameters** form in Communication Manager.

Table 33: Field values and descriptions for Restrict Calls

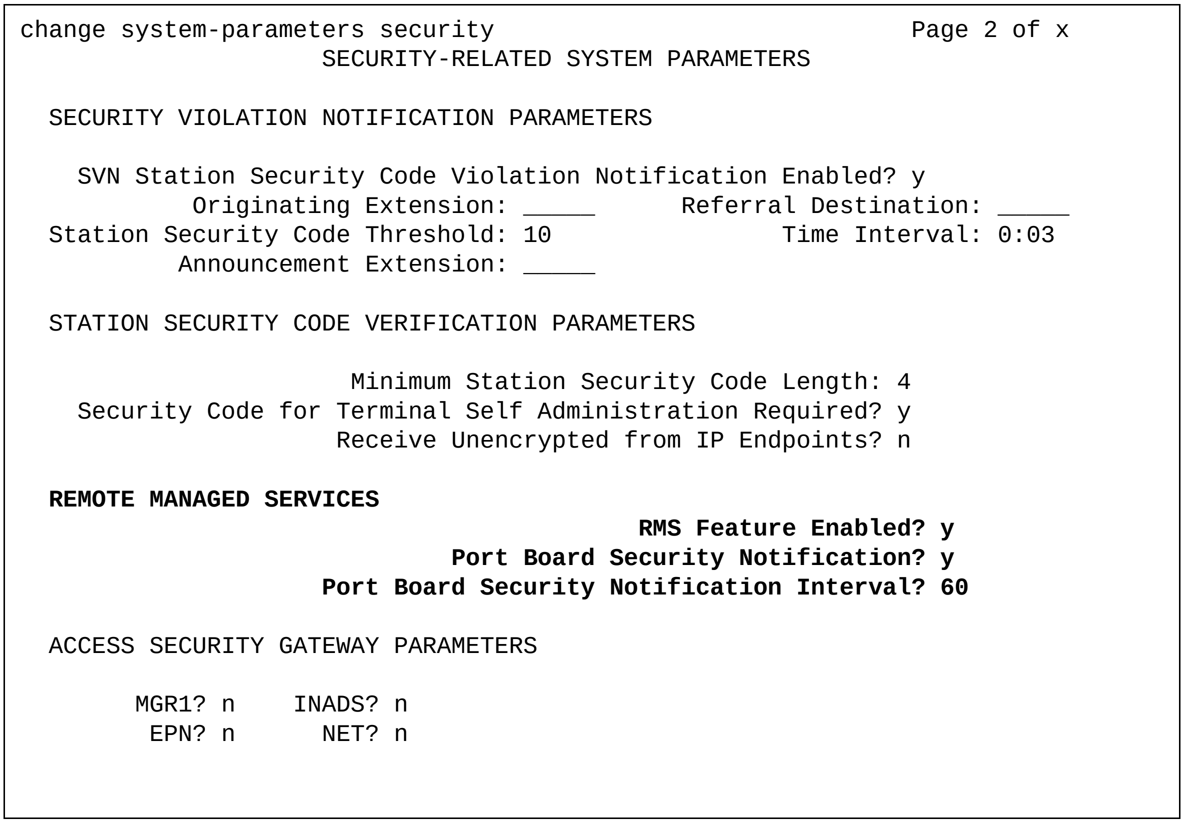
Field value	Direction	Description
stations-first	Inbound	Denies new traffic generated by internal stations, allowing inbound calls only (best for call center environments).
all-trunks-first	Outbound	Denies all outbound calls to trunks, tie-lines, and stations, and all station-originated calls.
public-trunks-first	Inbound	Denies all inbound calls from trunks and tie-lines.

Remote Managed Services

This feature provides notification of security-related events by generating SNMP traps that are forwarded to the Security Operations Center (SOC). Security traps correspond to the following events:

- G250, G350, G430 or G450 Media Gateway or a C-LAN or MEDPRO that:
  - Detects DoS attacks
  - Registers (goes into service), de-registers (goes out of service), or resets
- IP endpoint or Enterprise Mobility User (EMU) that attempts to register with an invalid PIN or non-existent extension
- IP endpoint that registers (goes into service), de-registers (goes out of service), or resets

Administer Remote Managed Services at the Communication Manager SAT interface with the **`change system-parameters`** ***`security`*** command.



```
change system-parameters security                             Page 2 of x
                    SECURITY-RELATED SYSTEM PARAMETERS

  SECURITY VIOLATION NOTIFICATION PARAMETERS

    SVN Station Security Code Violation Notification Enabled? y
            Originating Extension: _____      Referral Destination: _____
  Station Security Code Threshold: 10                Time Interval: 0:03
           Announcement Extension: _____

  STATION SECURITY CODE VERIFICATION PARAMETERS

                       Minimum Station Security Code Length: 4
    Security Code for Terminal Self Administration Required? y
                      Receive Unencrypted from IP Endpoints? n

  REMOTE MANAGED SERVICES
                                          RMS Feature Enabled? y
                            Port Board Security Notification? y
                   Port Board Security Notification Interval? 60

  ACCESS SECURITY GATEWAY PARAMETERS

        MGR1? n    INADS? n
         EPN? n      NET? n
```

Note:

The **RMS Feature Enabled** field default value is n(o), meaning that the Remote Managed Service feature is disabled. The example above shows the field enabled allowing the two fields below it to display.

Use the recommendations in Table 34: Denial of Service attack notifications through Managed Security Services on page 159 to alert you of security-related events, including DoS conditions.

Table 34: Denial of Service attack notifications through Managed Security Services

Field	Value	Recommendation
RMS Feature Enabled	**y/n**	Use this field to enable Remote Managed Services. When you set this field to **y**, the **Port Board Security Notification** and **Port Board Security Notification Interval** fields appear. Default is **n**.
		1 of 2

Table 34: Denial of Service attack notifications through Managed Security Services

Field	Value	Recommendation
Port Board Security Notification	**y/n**	Enter **y** to enable port board Denial of Service notification. Default is **n**. When you enter **y** in this field, the **Port Board Security Notification Interval** field appears.
Port Board Security Notification Interval	**60** to **3600** in increments of 10	Enter the desired interval (in seconds) between port board Denial of Service notifications (traps). Default is **60** (1 minute). **NOTE:** There is no delay before the first trap is sent. The interval administered in this field applies only to the period *between* traps.
		2 of 2

Signaling groups

Specifying both ends of a signaling group is crucial to a secure connection. Incomplete administration of the connection, that is, not specifying both the near- and far-end IP addresses prevents an attacker from accessing the signaling group connection and, thus, the call setup data. Communication Manager administration warns you of Denial of Service vulnerabilities if both ends of the connection are not administered.

To administer a signaling group:

1. The System Access Terminal (SAT) command **`add signaling-group`** ***`next`*** displays the Signaling Group administration form to create a new signaling group; use **`change signaling-group <`*`grpnum`*`>`** to edit an existing signaling group (**<*grpnum*>** is the number of a previously-administered signaling group.

   Note:
   The **Group Type** field must be either **h.323** or **sip**.

2. Use the recommendations in Table 35: Mitigating Denial of Service attacks through signaling group administration on page 161 to avoid DoS vulnerabilities from incomplete SIP or H.323 signaling group administration on the Signaling Group form

Table 35: Mitigating Denial of Service attacks through signaling group administration

Signaling group field	Group Type	Field value	Description
Far-end Domain	**sip**	40-character string	This field specifies the IP domain for which the far-end proxy is responsible (that is, authoritative), if it is different from the near-end domain. If the domains are the same, leave this field blank.
		blank	No warning.
Far-end Listen Port	**h.323** or **sip**	**1-65535**	Use the same value as the **Near-end Listen Port** field. For SIP over TLS the default value is **5061**.
		blank	If you leave this field blank, the system warns you that an unspecified far-end IP address is vulnerable to DoS attacks.
Far-end Node Name	**sip**	Administered node name	Enter the node name for the far-end Control LAN (C-LAN) IP interface used for trunks assigned to this signaling group. The node name must already be administered on the **IP Node Names** form.
		blank	If you leave this field blank, the system warns you that an unspecified far-end IP address is vulnerable to DoS attacks.

More information

- Interpreting the Security Violations Status reports on page 176

Chapter 5: Operational Security

Avaya Security Advisories

What is an Avaya Security Advisory

The Avaya Product Security Support Team (PSST) is responsible for the following:

- Managing Avaya product vulnerabilities and threats
- Maintaining information posted at http://support.avaya.com/security.
- Performing security testing and auditing of Avaya's core products
- Resolving security-related field problems in support of Avaya Global Services
- Managing the securityalerts@avaya.com mailbox.

As a result, the PSST actively monitors security issues related to the following topics:

- Avaya products
- Products that are incorporated into Avaya products
- General data networking and telecommunications, as identified by government agencies

When a security vulnerability is identified, the PSST determines susceptibility of Avaya products to those vulnerabilities and assigns one of four risk levels: **High, Medium, Low**, and **None** (see How to interpret an Avaya Security Advisory on page 165). Depending on the category of risk, the PSST creates an Avaya Security Advisory to notify customers of the vulnerability.

Depending on the vulnerability and its risk level, the advisory might include a recommended mitigation action, a recommendation regarding the use of a third-party provided patch, a planned Avaya software patch or upgrade, and/or additional guidance regarding the vulnerability.

How do I get Avaya Security Advisories?

Avaya Security Advisories are posted on the Security Support Web site at http://support.avaya.com/security. The PSST also sends email to customers who have signed up to receive advisories. The advisories are distributed in a time frame as indicated in Table 36: Avay Security Advisories time frames on page 164:

Table 36: Avay Security Advisories time frames

Avaya classification of vulnerability	Target intervals between assessment and notification
High	Within 24 hours
Medium	Within 2 weeks
Low	Within 30 days
None	At Avaya's discretion

Customers can sign up to receive advisories by email on the Avaya Security Support Web site by following these steps:

1. Browse to http://support.avaya.com.

2. Select **My E-notifications** on the right side of the page.

3. If you do not have an account click on **Registration Now** and follow the instructions.

4. Log in using your existing credentials.

5. Select **Add New E-notifications**.

6. Click **Submit.**

7. Select **Security Advisories** and click **Continue** to receive notifications on creation or update of all security advisories.

   To receive notification on creation or update of security advisories of a specific product select a product from the product list and skip to step 9.

8. Select **Security Advisories** and click **Submit** to ensure that **E-notifications** is added. Skip to step11.

9. From the release version page select the product version and click **Continue**.

10. Select **Security Advisories** in **Avaya Support E-Notifications Service** page and click **Submit**.

11. A confirmation page appears.

    You are now ready to receive email E-Notifications whenever an Avaya Security Advisory is updated or published.

How to interpret an Avaya Security Advisory

Precise definitions that the Avaya Product Security Support Team (PSST) follows in classifying vulnerabilities relative to their potential threat to Avaya products is in *Avaya's Security Vulnerability Classification* document (http://support.avaya.com/elmodocs2/security/security_vulnerability_classification.pdf).

Table 37: Avaya's security vulnerability classification on page 166 summarizes the three main categories.

Table 37: Avaya's security vulnerability classification

Vulnerability classification	Criteria for classification
High	The product is vulnerable to: ● Attacks from a remote unauthenticated user who: – Can easily access high-level administrative control of a system or critical application without interaction with a user of the product beyond standard operating procedures. ● Attacks from remote unauthenticated user who: – Can easily cause the system or a critical application to shutdown, reboot, or become unusable without requiring interaction with a product user. For example, see the advisory at http://support.avaya.com/elmodocs2/security/ASA-2006-002.htm.
Medium	The product does not meet criteria for high vulnerability, but is vulnerable to: ● Attack from a user who can access a user account, and access does not directly require the privileges of a high-level administrative account. ● The system and/or critical application shutting down, rebooting, or becoming unusable, and an existing administrative or local account is used for this attack. ● Attack from a user who can access a local user account from which higher-level privileges are available. For example, see the advisory at http://support.avaya.com/elmodocs2/security/ASA-2006-262.htm
Low	The product does not meet criteria for medium or high vulnerability, but is vulnerable to: ● Compromise of the confidentiality, integrity, or availability of resources, although any compromise is difficult or unlikely without non-standard direct user interaction. ● Non-critical applications shutting down, rebooting, or becoming unusable. For example, see the advisory at http://support.avaya.com/elmodocs2/security/ASA-2007-015.htm.
None	A related third-party product has a vulnerability but the affected software package(s), module(s), or configuration(s) are not used on an Avaya product and there is therefore no vulnerability. For example, see the advisory at http://support.avaya.com/elmodocs2/security/ASA-2006-261.htm.

How an advisory is organized

Each Avaya Security Advisory contains the following information:

- **Overview** — A description of the vulnerability.

  For operating system or third-party software, a link is also provided for quick access to a Web site for more information. The linked information provides:

  - A description of the risk
  - Instructions on how to correct the problem, which might include:
    - Installing an update
    - Revising administration of the product
  - A description of what additional security fixes, if any, are included in the update.

- **Avaya Software-Only Products** — A listing of the specific Avaya products that use, but are not bundled with, operating system software that might be vulnerable. Information includes:
  - The product version affected
  - Possible actions to take to reduce or eliminate the risk

- **Avaya System Products** — A listing of the specific Avaya products that are vulnerable or are bundled with operating system software that might be vulnerable. Information includes:
  - The level of risk
  - The product version affected
  - Possible actions to take to reduce or eliminate the risk

- **Recommended Actions** — A list and description of steps to take to remove the vulnerability. The steps might include installing a security update, administering a security feature, or performing a software upgrade. For operating system and third-party software, the recommended actions are normally identified in detail through the Web site links in the security advisory.

How Avaya incorporates security updates in its applications

When a third-party update (also called a patch) is available to mitigate a security vulnerability, Avaya might recommend that the customer apply the patch from the third-party. This action, if recommended, is stated explicitly in the Avaya Security Advisory.

For some third-party updates, Avaya might not recommend installation due to interoperability, stability, or reliability issues with the update and Communication Manager. In this case, before Avaya releases a security update, Avaya thoroughly tests it on a non-production system, along with all the other software that is normally loaded (and not loaded) on a Communication Manager server. Sometimes Avaya must modify the update before it works correctly. Customers who apply third-party provided patches without Avaya's recommendation might void their warranty.

In some instances, when a software vendor provides an update to address a vulnerability, Avaya might decide to address the vulnerability through other means to avoid potential risks to Communication Manager. This might include modification of existing software through an Avaya-issued update which is released separately or incorporated into future releases of the product. Such decision to offer an alternative remediation is described in the advisory.

Logging, monitoring and audit trails

Removing old accounts

Remove unused administrator accounts to help prevent unauthorized access to sensitive logs and files. Communication Manager System Management Interface allow you to add, change, lock, or remove administrator logins and login groups for the server. Web pages do not manage logins that are authenticated in an external server such as LDAP.

Remove administrator accounts on the **Security > Administrator Accounts** page as described in *Avaya Aura™ Communication Manager Feature Description and Implementation (555-245-205)*.

Restricting web access to system logs

Define permissions for access to Communication Manager Web pages and system logs through the System Management Interface by creating or editing a profile on the **Security > Web Access Mask** page.

For more information see:

- System Management Interface default profiles and permissions on page 33 for the default permission setting for Profile 18 (superuser) and Profile 19 (user).
- A complete discussion of the **Web Access Mask** page is in *Avaya Aura™ Communication Manager Feature Description and Implementation (555-245-205)*.

Where is security information logged?

Security information is logged in or notified through:

- SNMP trap receiver (see Configuring SNMP and syslog on page 116)
- Syslog security log (see Configuring the syslog server in Communication Manager on page 123)
- Miscellaneous logs (viewed from the Systems Log page, Figure 17: System Logs page on page 130) that track security-related information:
  - Linux access security log
  - Platform command history log
  - HTTP/web access log
  - IP events
  - Platform bash command history log
  - Communication Manager’s SAT events

Reading and interpreting the security logs

Both the Linux syslog and the Communication Manager application log security-related events.

Topics in this section include:

Interpreting the syslog header

Each syslog entry has a common header format:

```
yyyymmdd:hh:mm:sssss text
```

Table 38: Syslog entry header format description

Variable	Description
yyyy	The year
mm	The month of the year
dd	The day of the month
hh:mm:sssss	The time in 24-hour format
text	The log event text as supplied by the event source module. A module name, process ID, and priority are the leading portion of this text string.

Syslog header example

```
20070326:061058000:7103:cmds:MED:
```

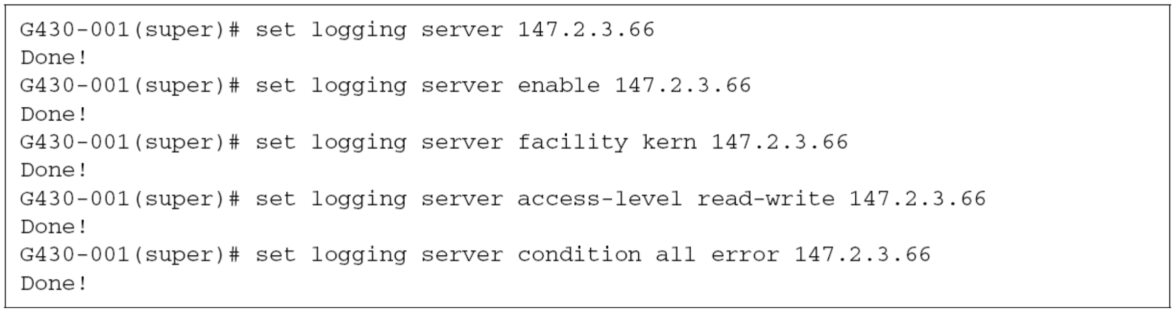
- **Date**: March 26, 2007
- **Time**: 06:10:58 (AM)
- **Text**: 7103:cmds:MED:

Syslog server example for a branch gateway

The following example defines a Syslog server of G430 gateway with the following properties:

- IP address `147.2.3.66`
- Logging of messages enabled
- Output to the Kernel facility
- Only messages that can be viewed by read-write level users are received
- Filter restricts receipt of messages from all applications to those less severe than error

Figure 25: Syslog server for G430 gateway



```
G430-001(super)# set logging server 147.2.3.66
Done!
G430-001(super)# set logging server enable 147.2.3.66
Done!
G430-001(super)# set logging server facility kern 147.2.3.66
Done!
G430-001(super)# set logging server access-level read-write 147.2.3.66
Done!
G430-001(super)# set logging server condition all error 147.2.3.66
Done!
```

Interpreting SNMP entries in the syslog

The SNMP agent logs security events to syslog *local0* in the following format (following the syslog header):

```
module-name[pid]: snmp ip R set object | value
```

Table 39: SNMP agent log description

Log entry	Description
module-name	The name of the SNMP module logging the event
pid	The Linux process ID of the process initiating the log entry
snmp	The text string "snmp"
ip	The ip address of the management system
R	Result codes: ● s: action was successful ● f: action failed for non-security reason ● v: action failed due to a security violation Note: An ASCII error code might follow the letter "f" and an optional colon (:), for example, "f:123456."
set	The string "set"
object	A human readable name for the object being accessed
value	The new value for the object being set.

SNMP log example

```
some-module[12345]: snmp 192.11.13.5 s set loadipsi /var/home/ftp/
pub/tn2312ap_f21.tar
```

Note:

Only "sets" are logged, "gets" are not.

SNMP agents log a single asterisk (*) for any passwords, pins, encryption keys, or security tokens, if any.

Interpreting the platform command history log

The following general format is used for all log entries in the Platform command history log (following the syslog header):

```
mmm dd hh:mm:ss server-name text
```

Table 40: Platform command history log descriptions

Field	Description
mmm	The month in text format, for example "Aug"
dd	The day of the month
hh:mm:ss	The time in 24-hour format
server-name	The host name of this server
text	The text field contains the log event text that is supplied by the module logging the event. For more information on the text field see the following sections: ● Interpreting the command history log for Communication Manager SAT on page 177 ● Interpreting the command history log for Web activity on page 180

Platform command history log example

```
20070326:061058000:7101:cmds:MED:server-name -bash: HISTORY:
PPID=23691 PID=23692 UID=778 productid

20070326:061058000:7103:cmds:MED:server-name -bash: HISTORY:
PPID=23691 PID=23692 UID=778 almcall

20070326:061058000:7104:cmds:MED:server-name -bash: HISTORY:
PPID=23691 PID=23692 UID=778 almenable

20070326:061058000:7105:cmds:MED:server-name -bash: HISTORY:
PPID=23691 PID=23692 UID=778 serialnumber
```

Each of the four Linux platform command log entries ends with the command that was issued at the Linux command line interface (CLI): **`productid`**, **`almcall`**, **`almenable`**, and **`serialnumber`**.

Interpreting Communication Manager security violations

SAT command and syntax

Use the **`monitor security-violations`** from the Communication Manager system access terminal (SAT) to see the following information about failed attempts to access the system:

- the time of the violation
- the login entered
- the port accessed during the failed login attempt

Remote access violations contain additional information:

- trunk-group number
- member number
- extension

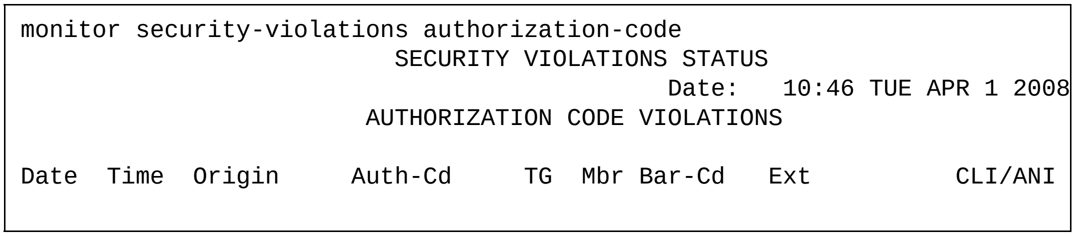
A total of 16 entries are maintained for each type of access. Security violation reports are automatically updated every 30 seconds until the command is canceled by pressing **CANCEL**. Canceling does not log off the terminal.

⚠ **Important:**
The **RMS Feature Enabled** field on page two of the **Security-Related System Parameters** form (**`change system-parameters security`**) must be set to **`y`** before the **`monitor security-violations`** command will run (see Remote Managed Services on page 158).

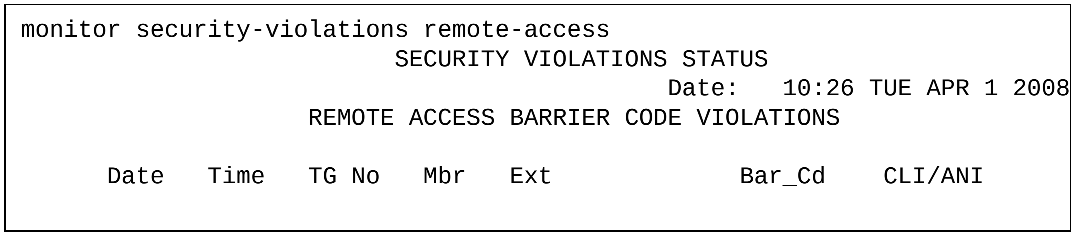
Action/Object	Qualifier	Qualifier Description	Logins
`monitor security-violations`	**`authorization-code`** **`remote-access`** **`station-security-codes`**	Monitors system access. Monitors remote system access. Monitors phone (station) access.	init inads craft cust rcust bcms browse

Interpreting the Security Violations Status reports

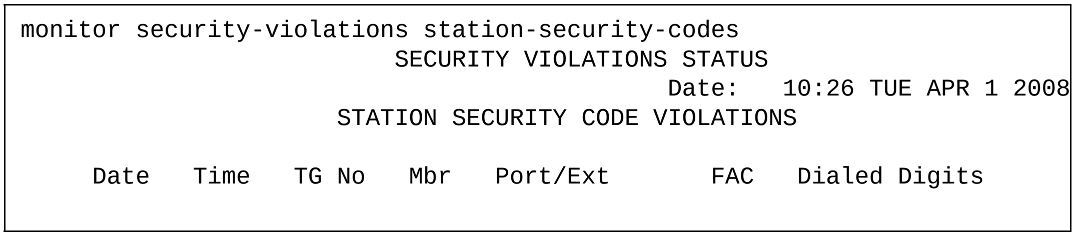
Depending on the command qualifier, the Security Violations Status reports differ slightly. Field descriptions are in Security Violations Status field descriptions on page 176.



```
monitor security-violations authorization-code
                          SECURITY VIOLATIONS STATUS
                                             Date:   10:46 TUE APR 1 2008
                        AUTHORIZATION CODE VIOLATIONS

Date  Time  Origin     Auth-Cd     TG  Mbr Bar-Cd   Ext          CLI/ANI
```



```
monitor security-violations remote-access
                          SECURITY VIOLATIONS STATUS
                                             Date:   10:26 TUE APR 1 2008
                    REMOTE ACCESS BARRIER CODE VIOLATIONS

      Date   Time   TG No   Mbr   Ext             Bar_Cd    CLI/ANI
```



```
monitor security-violations station-security-codes
                          SECURITY VIOLATIONS STATUS
                                             Date:   10:26 TUE APR 1 2008
                      STATION SECURITY CODE VIOLATIONS

     Date   Time   TG No   Mbr   Port/Ext       FAC   Dialed Digits
```

Table 41: Security Violations Status field descriptions *1 of 2*

Date	The date of the security violation (MM/DD)
Time	The time of the logged security violation (HH:MM)
Origin	___________________________________ (authorization violations only)
Auth-Cd	The failed authorization code that generated the security violation (authorization violations only)
TG TG No	Trunk group through which the security violation occurred The trunk group number that carried the incoming access attempt
Mbr	Trunk group member through which the security violation occurred
	1 of 2

Table 41: Security Violations Status field descriptions *2 of 2*

Ext	Extension number through which the security violation occurred
Port/Ext	The type of port and extension through which the security violation occurred
Bar-Cd	Bar code of the physical equipment used (authorization violations only)
FAC	Feature Access Code (FAC) used (station violations only)
CLI/ANI	
Dialed Digits	
	2 of 2

Interpreting the command history log for Communication Manager SAT

Depending on the level of logging that is enabled, the format for the text portion of log entries for the Communication Manager SAT (following the syslog header) is:

```
module-name[pid]: sat sid uid uname profile R action object
qualifier fieldName | oldValue | newValue
```

Table 42: Communication Manager SAT command history log format on page 177 lists and describes the text formats in the log entry for SAT.

For more information about logging levels see Administering logging levels in Communication Manager on page 126.

Table 42: Communication Manager SAT command history log format

Field	**Description**
module-name	The name of the software module that created the entry in the log
pid	The Linux process ID that created the entry in the log
	1 of 2

Table 42: Communication Manager SAT command history log format

Field	**Description**
sat	The text string "sat" identifies a Communication Manager SAT log entry.
sid	The parent process ID of the autostat process, or the process ID of the TUI process associated with this SAT session when this SAT session was through a C-LAN.
uid	The SAT user's numeric ID
uname	The SAT user's login name
uname2	The SAT user's secondary login name
profile	The access profile number that is assigned to this user
R	The status of the action: ● **s**: the action was a success ● **f**: the action was a failure other than for a security reason. An ASCII error code might follow the letter "f" and an optional colon (:), for example, "f:123456." ● **v**: the action was a failure due to a security violation.
action	The SAT command invoked by the user, for example **`add`**, **`display`**, and **`list`**
object	The SAT form that was accessed, for example, station, trunk-group, etc.
qualifier	Contains the instance of the form or object. For example, in the **`display station`** ***`1000`*** command the qualifier is "1000."
fieldName	The name of the field in the SAT form
oldValue	The value of the field before the change
newValue	The value of the field after the change
	2 of 2

SAT log example

⚠ **SECURITY ALERT:**
Authorization codes, PINs, encryption keys, and passwords never appear in the command history log.

- Commands that do not change data only log the form invocation:

  module-name[98765]:sat 13533 778 login login 0 s display station 1000

  This log entry indicates that the user accessed the station form for extension 1000 but did not make any changes.

- One log entry is created for the form invocation and one log entry is created for each field that was changed for commands that change one or more fields within a form:

  module-name[98765]: sat 13533 778 login login 0 s display station 1000

  module-name[98765]: sat 13533 778 login login 0 s change station 1000 Name | Joe Smith | Mary Jones

  module-name[98765]: sat 13533 778 login login 0 s change station 1000 Security Code | * | *

  module-name[98765]: sat 13533 778 login login 0 s change station 1000 Coverage Path 1 | 3 | 6

  module-name[98765]: sat 13533 778 login login 0 s change station 1000 Personalized Ringing Pattern 1 | 2 | 4

  These entries indicate the following:

  - The name associated with extension 1000 changed from "Joe Smith" to "Mary Jones."
  - The security code for extension 1000 changed, but the security codes (indicated by "*") do not display in the log.
  - The **Coverage Path 1** field for station 1000 changed from 3 to 6.
  - The **Personalized Ringing Pattern 1** field for station 1000 changed from 2 to 4.

Note:
For commands that log new entries, only values that change from a default value are logged.

Interpreting the command history log for Web activity

Depending on the information on a Web page, the text formats for log entries (following the syslog header) of Web activity are:

```
module-name[pid]: web ip uid uname profile R page-name

module-name[pid]: web ip uid uname profile R page-name | button |
button-name

module-name[pid]: web ip uid uname profile R page-name |
variable-name | value
```

Table 43: Abbreviated Dialing Button Programming command history log format on page 180 lists and describes the text formats in the log entry for Web activity.

Table 43: Abbreviated Dialing Button Programming command history log format

Field	Description
module-name	The name of the software module that created the entry in the log
pid	The Linux process ID that created the entry in the log
web	The text string "web" to indicate a web log entry.
ip	The IP address of the user accessing the server
uid	The ID number of the user establishing the Web session
uname	The login name for the user establishing the Web session.
profile	The access profile number assigned to the user
R	The status of the action: ● **s**: the action was a success ● **f**: the action was a failure other than for a security reason. An ASCII error code might follow the letter "f" and an optional colon (:), for example, "f:123456." ● **v**: the action was a failure due to a security violation.
page-name	The name of the page that the user accessed
button	The text string "button" to indicate that the next value is the button-name.
button-name	The button label as shown on the form
	1 of 2

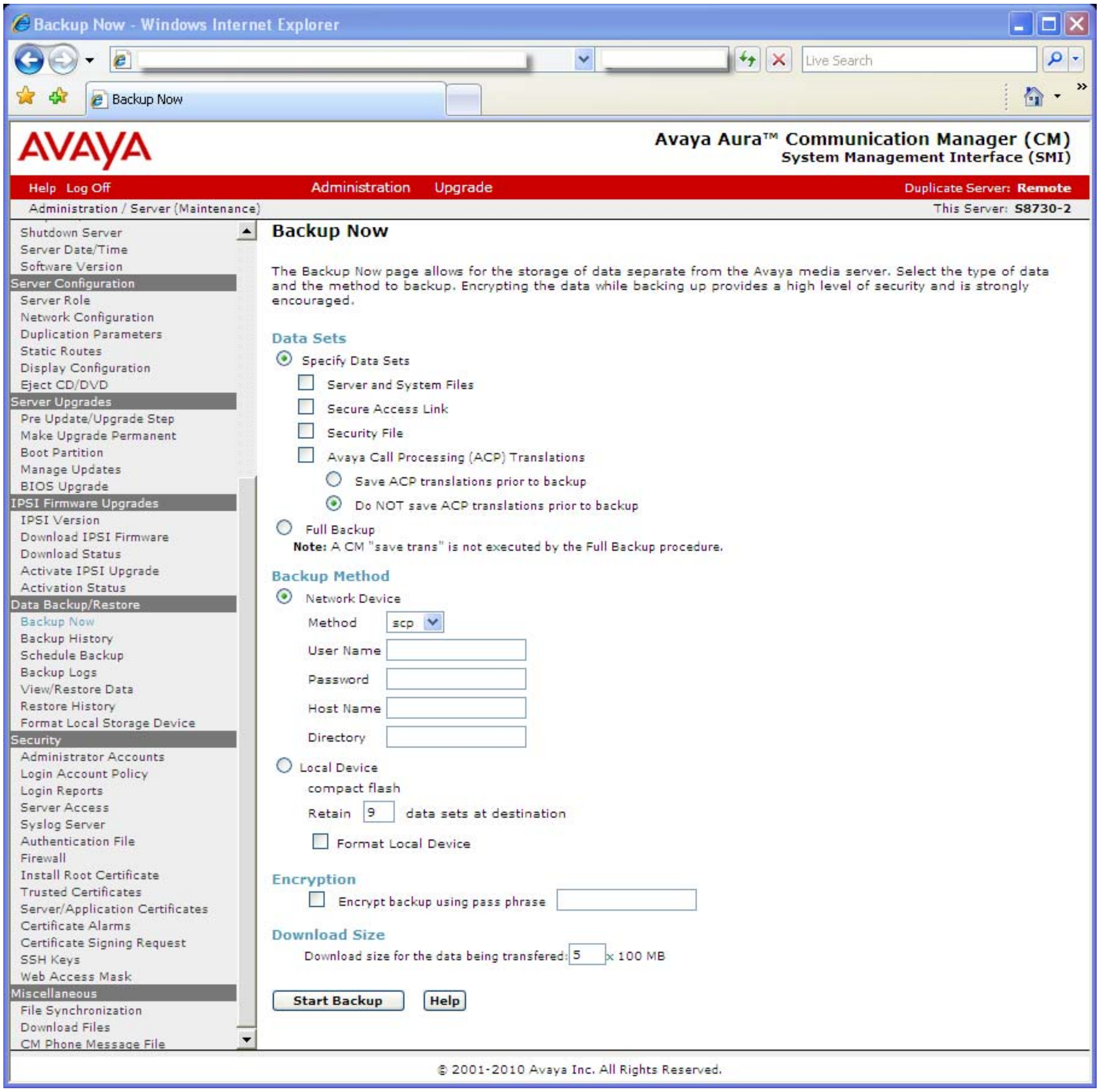
Table 43: Abbreviated Dialing Button Programming command history log format

Field	Description
variable-name	The name of the text box, button, or check box on the form
value	The value of the variable name after the change. In instances where the variable name is the name of a check box, the value is "checked" or "unchecked."
	2 of 2

Web log entry example

For example, consider the **Backup Now** page shown in Figure 26: Backup Now page with initial defaults on page 182 (the page as it is initially presented to the user).

Figure 26: Backup Now page with initial defaults



Backup Now

The Backup Now page allows for the storage of data separate from the Avaya media server. Select the type of data and the method to backup. Encrypting the data while backing up provides a high level of security and is strongly encouraged.

Data Sets

● Specify Data Sets
- □ Server and System Files
- □ Secure Access Link
- □ Security File
- □ Avaya Call Processing (ACP) Translations
  - ○ Save ACP translations prior to backup
  - ● Do NOT save ACP translations prior to backup

○ Full Backup
Note: A CM "save trans" is not executed by the Full Backup procedure.

Backup Method

● Network Device
- Method: scp
- User Name:
- Password:
- Host Name:
- Directory:

○ Local Device
- compact flash
- Retain 9 data sets at destination
- □ Format Local Device

Encryption

□ Encrypt backup using pass phrase

Download Size

Download size for the data being transfered: 5 x 100 MB

Start Backup | Help

© 2001-2010 Avaya Inc. All Rights Reserved.

Then the user makes the following changes:

- Un-checks the box labeled "Avaya Call Processing (ACP) Translations"
- Checks the box labeled "security files"
- Selects SCP and enters appropriate data

The log entries created (following the syslog header) are similar to the following:

```
some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now

some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now |
acp xln | uncheck

some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now |
security files | check

some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now |
ftp | check

some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now |
user name | backupoperator

some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now |
password | *

some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now |
hostname | dataserver

some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now |
directory | /cm

some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now |
button | start backup
```

Only the first event is logged unless the user clicked the **Start Backup** button. Field changes are not logged unless the page is actually submitted. The field name "Avaya Call Processing (ACP) Translations" is abbreviated to try to make the log entry as short as possible, yet still recognizable.

Software and firmware updates

How Avaya delivers security updates

Generally, Avaya makes security updates available on or through the Avaya Security Web site at http://support.avaya.com/security. In addition, Avaya incorporates security updates, if applicable, in subsequent software release packages.

Based on the classification of vulnerability and the availability of a vendor-supplied update, Avaya makes a best effort attempt to provide remediation actions based on the following target intervals:

Table 44: Vulnerability classifications and remediation intervals

Vulnerability	Target remediation intervals
High	If Avaya needs to develop a software update, the Avaya Security Advisory provides a timeline for availability of the update. Avaya incorporates the fix into a separate service pack or update (30 days maximum delivery time). If a software patch is available for installation or another action is recommended, the Avaya Security Advisory describes the actions.
Medium	If Avaya needs to develop a software update, Avaya includes the update in the next major release that can reasonably incorporate the update. If no new major releases are scheduled for a product, and Avaya is providing maintenance support, Avaya incorporates the fix into a separate service pack or update (1 year maximum delivery time). If a software patch is available for installation or another action is recommended, the Avaya Security Advisory describes the actions.
	1 of 2

Vulnerability	Target remediation intervals
Low	If Avaya needs to develop a software update, Avaya includes the update in the next major release that can reasonably incorporate the update. If no new major releases are scheduled for a product, and Avaya is providing maintenance support, Avaya incorporates the fix into a separate service pack or update (1 year maximum delivery time). If a software patch is available for installation or another action is recommended, the Avaya Security Advisory describes the actions.
None	No remediation actions are required.
	2 of 2

Avaya product development staff incorporates a third-party update into its software in one of three ways:

- Avaya simply bundles the specific update or the new release of the affected software with the Communication Manager software such that the security-related updates are automatically incorporated into the Avaya product operation.
- Avaya modifies the Communication Manager software so that the specific update or the new release of the affected software is appropriately incorporated into the Communication Manager operation.
- Avaya modifies the specific update or the new release of the affected software so that the security-related updates are automatically incorporated into the Communication Manager operation.

When Avaya incorporates one or more security fixes into its software, the fixes might be delivered in one of three forms:

- A security update

  A security update includes operating system and/or third-party software security fixes.
- An Avaya software update

  An Avaya software update includes software security fixes to the Avaya application software.

- An Avaya full release of software

  An Avaya full release of software includes all software for the Avaya product, including software security fixes to the Avaya application software and/or security fixes for the operating system and third-party fixes.

Validating a security update

When Avaya determines that a third-party security update applies to one or more of its products, Avaya product development tests the update on the affected current products to ensure there are no adverse affects to the published functionality of the products. In addition, when third-party updates are included in new software releases, the products are thoroughly tested.

Avaya-generated security updates are likewise tested on all affected products prior to release. Avaya security updates are likewise tested before incorporation into subsequent releases.

Testing meets requirements of internal Avaya testing standards, including testing for the following:

- Denial of Service
- Encryption standards
- Certificate management
- Audits and logging
- Access control

Applying an operating system security update

Operating system security updates for Communication Manager servers are typically applied separately from other platform or Communication Manager software updates. If Avaya issues a security update, the customer might apply the update themselves or engage their service support group to apply it.

Instructions for applying a security update are normally provided either in the security advisory or as instructions on the Web site for updates of the associated operating system or application package. See http://support.avaya.com/security.

For Communication Manager, the Manage Updates Web pages facilitate applying the security updates. See “Installing security and Communication Manager service pack updates” in *Installing and Upgrading the Avaya S8300 Server (555-234-100).*

Applying an Avaya field load or software update

An Avaya field load, or software update, is an update of the Avaya product software. In some cases, a security-related change to Avaya software may result in the creation of a Communication Manager software update.

If Avaya issues an Avaya software update, the customer might apply the update themselves or engage their service support group to apply it. In most cases, the customer is responsible for applying the update unless the customer’s Maintenance contract includes automatic software updates. In some cases, only services personnel have permission to apply the update.

Software updates are posted on the Avaya Download Center. An Avaya customer must register with the Download Center to obtain a login, and then the customer can access the Avaya update software applicable to the customer’s products. Instructions for applying a security update are normally provided either in the security advisory or as instructions on the Download Software Web site.

For Communication Manager, the System Management Interface facilitates applying a software update. In such cases, product documentation, as well as the associated security advisory, describes how to use the interface to install the update. See “Installing security and Communication Manager service pack updates” in *Installing and Upgrading the Avaya S8300 Server (555-234-100).*

Determining the contents of a security update

For each security update for a third-party application or the Linux operating system, the referencing security advisory provides a link for quick access to the third-party Web site. Such Web sites typically provide a description of the security fixes that are included in the update.

For a security update for Communication Manager, the referencing security advisory provides a link to an Avaya Web page or FTP site that stores the update and a readme file that describes the security fixes in the update.

Avaya may package multiple third-party security updates together for installation on Communication Manager. Such packages are cumulative and include all security updates previously available and applicable to the product. In many cases, once the package is installed, the customer can use Communication Manager’s Manage Software Web page to locate the update file name.

The customer can then determine the contents with the following steps:

1. Access the Avaya support Web page at http://support.avaya.com.
2. Select Download Software.
3. Select Communication Manager.
4. Select **Latest TN Circuit Pack, Media Server, and Media Gateway Firmware and Software Updates**.
5. Select the appropriate G.A. load of Communication Manager software.
6. Select the **Latest S8x00 Media Server Service Pack Update Contents**.
7. Select **Contents of Latest Service Pack for S8500**.
8. View the readme file for the security update package.

In Communication Manager Release 4 or higher, the customer can run the Linux command **`update_info`** ***`<security patch name>`***, where ***`<security patch name>`*** is the name of the Avaya security update. The resulting display identifies each Avaya security advisory number. The customer can then access the Avaya Security Web page and view the contents for each security advisory.

Regulatory issues

- Considerations for customers who must comply with the Sarbanes-Oxley Act on page 189
- Considerations for customers who must comply with the Graham-Leach-Bliley Act on page 192
- Considerations for customers who must comply with HIPAA on page 193

- Considerations for customers who must comply with CALEA on page 194
- Considerations for customers who must comply with FISMA on page 196
- Considerations for customers who want to comply with ISO 17799 on page 197
- Considerations for customers who must comply with E911 on page 200
- Considerations for non-US customers who must comply with regulations on page 202

Considerations for customers who must comply with the Sarbanes-Oxley Act

Note:

This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the act's requirements. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The Sarbanes-Oxley Act of 2002 is a federal law enacted in response to a number of accounting scandals involving major U.S. corporations. A key requirement of the act is that public companies evaluate and disclose the effectiveness of their internal controls as they relate to financial reporting. One major area of internal control consists of information technology controls. As a result, the Sarbanes-Oxley Act holds chief information officers responsible for the security, accuracy and the reliability of the systems that manage and report the financial data.

To the extent that a company uses data collected or transmitted by Communication Manager as part of its overall cost or revenue reporting and financial management, the company can use security-related features of Communication Manager to secure the data. Use of these features can further demonstrate the company's good faith data management and reporting.

Communication Manager security features also help prevent unauthorized access to the customer's network, in general.

See Table 45: Data security features in this guide on page 190 for features related to data security and documented in more detail in other sections of this document.

Table 45: Data security features in this guide

Feature	How related to Sarbanes-Oxley	Where documented
Encryption	Transmitted data is protected from packet-sniffing and eavesdropping	See: ● Avaya's encryption overview on page 43
Access control	Access to data is protected from unauthorized personnel	See: ● Access profiles on page 32 ● Managing administrative accounts on page 110
Authentication	Access to the system is restricted by login/password.	See: ● Access profiles on page 32 ● Managing administrative accounts on page 110
Logging	Security-related events are logged	See: ● Configuring SNMP and syslog on page 116 ● Reading and interpreting the security logs on page 170
Backup of data	Data saved on backup media or backup server. Protected by encryption and key.	See: ● Secure backups of Communication Manager data and translations on page 204

Communication Manager data used for financial purposes

Communication Manager can generate call detail records that might be used in financial data:

- Communication Manager generates call detail records in real-time and sends the records to a device the customer specifies. The device can be a printer or a reporting system that converts call record data into financial records. Two such reporting systems, eCAS Call Accounting System and VeraSmart Application Suite, are available through Avaya DeveloperConnect partner Veramark Technologies, Inc. These devices provide their own data security. For more information, see http://www.veramark.com/products/verasmart.htm.

- Communication Manager transmits Call Detail Recording (CDR) records to call accounting devices over a TCP/IP connection using Avaya's proprietary Reliable Session Protocol. While the data are protected from corruption, the data are not encrypted. For this reason, where possible, the customer should cable the CDR device directly to the Communication Manager server, whenever possible, for the export of CDR data.

- The customer may add the following financial data elements for inclusion in CDR records:

  - Account codes are codes that users can manually enter identify the purpose or the associated client of each call. Communication Manager includes account codes in CDR records when account codes are enabled.
  - Advice of Charge (AOC, for ISDN trunks) is charge information that Communication Manager collects from the public network for each outgoing call. Charge advice is a number representing the cost of a call; it might be recorded as either a charging or currency unit.
  - Periodic Pulse Metering (PPM, for non-ISDN trunks) is data that Communication Manager based on the pulses transmitted from the public network at periodic intervals during an outgoing trunk call. At the end of the call, the number of pulses collected is the basis for determining charges.

Other adjunct systems collecting Communication Manager data

The Avaya Call Management System (CMS) and the Avaya Interactive Response system both collect call data that might be used to generate financial reports. Like the CDR reporting devices, these systems have a number of security features that can be used to protect data.

The CMS communicates with Communication Manager over a TCP/IP connection using a proprietary binary protocol. The Interactive Response system communicates with Communication Manager using a TCP/IP connection. The customer can enhance the Interactive Response connection by using TLS and SRTP protocols.

For more information on Interactive Response security, see http://support.avaya.com/elmodocs2/ir/r2_0/print_Security.pdf.

For more information on Call Management System security, see "Avaya Call Management System Security Whitepaper."

Considerations for customers who must comply with the Graham-Leach-Bliley Act

Note:

This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the act's requirements. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The Gramm-Leach-Bliley Act (GLB) requires financial institutions to disclose privacy policies regarding customer data. This disclosure must describe the ways the institution may use and disclose private information.

Where indicated in their policy, financial institutions must protect the privacy of their customers, including customers' nonpublic, personal information. To ensure this protection, the Graham-Leach-Bliley Act mandates that all institutions establish appropriate administrative, technical and physical safeguards.

Communication Manager data to which the Graham-Leach-Bliley Act might apply includes customer names and telephone numbers, called and calling number data, and abbreviated dial lists.

Use of the following key features can protect customer privacy and demonstrate the company's compliance with the interagency guidelines supporting the Graham-Leach-Bliley Act.

Table 46: Communication Manager security and compliance of Graham-Leach-Bliley Act

Feature	How related to Graham-Leach Bliley Act	Where documented
Encryption	Transmitted and stored data is protected from unauthorized individuals.	See: ● Avaya's encryption overview on page 43
System access control	Access to data is protected from unauthorized personnel.	See: ● Access profiles on page 32 ● Managing administrative accounts on page 110
		1 of 2

Feature	How related to Graham-Leach Bliley Act	Where documented
Authentication	Access to the system is restricted by login/password.	● Access profiles on page 32 ● Managing administrative accounts on page 110
Backup of data	Protection against destruction, loss, or damage of customer information due to potential environmental hazards or technological failures; protected by encryption and key	See ● Secure backups of Communication Manager data and translations on page 204
		2 of 2

Considerations for customers who must comply with HIPAA

Note:
This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the act's requirements. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires health care providers to disclose to health care recipients the ways in which the institution may use and disclose private information. HIPAA also requires health care providers to protect the privacy of certain individually identifiable health data for health care recipients.

Communication Manager data to which HIPAA might apply includes customer names and telephone numbers, and called and calling number data.

Use of the following key features can protect patient privacy and demonstrate the health care provider's compliance with HIPAA.

Table 47: Communication Manager security and compliance of HIPAA

Feature	How related to HIPAA	Where documented
Encryption	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate	See: ● Avaya's encryption overview on page 43
System access control	Implement technical policies and procedures for electronic information systems that maintain electronically-protected health information to allow access only to those persons or software programs that have been granted access rights.	See: ● Managing administrative accounts on page 110
Authentication	Implement procedures to verify that a person or entity seeking access to electronically-protected health information is the one claimed.	See: ● Access profiles on page 32 ● Managing administrative accounts on page 110
Backup of data	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronically-protected health information.	See: ● Managing administrative accounts on page 110

Considerations for customers who must comply with CALEA

Note:

This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the act's requirements. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

In response to concerns that emerging technologies such as digital and wireless communications are increasing the difficulty for law enforcement agencies to execute authorized surveillance, Congress enacted the Communication Assistance for Law Enforcement Act (CALEA) in 1994. CALEA is intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that the systems support the necessary surveillance capabilities of law enforcement agencies.

In an order effective September 23, 2005, the FCC concluded that CALEA applies to facilities-based broadband Internet access providers and interconnected VoIP service providers. To the extent that CALEA applies to Avaya offerings, such offerings have achieved compliance with the applicable CALEA requirements. In the event that an Avaya customer is subject to CALEA requirements, there are various third-party products, including Session Border Controller products, that claim to provide or facilitate CALEA compliance.

Examples of these products are:

- NexTone
- AcmePacket
- Sipera

In addition, Communication Manager characteristics that can aid in CALEA compliance are the following:

- Communication Manager use of standard architectures. For example:
  - Communication Manager uses Open Systems Interconnection (OSI) standards for network communications. Therefore, transmissions are interceptable for surveillance tools established to work with the OSI standards.
  - Communication Manager telephone calls are always divided into call control signaling and voice or bearer signaling. This simplifies the task of determining what data to surveil.
- Communication Manager assurance of the authenticity and integrity of the calls being surveilled through its encryption and authentication capabilities.
- Call Detail Records, which records called numbers, and other call data that might be useful to law enforcement.

Finally, Communication Manager offers the service observing feature, which allows monitoring of calls with or without awareness of the parties on the call.

Considerations for customers who must comply with FISMA

Note:
This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the act's requirements. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The Federal Information Security Management Act of 2002 provides for development and maintenance of minimum controls required to protect Federal information and information systems. Telecommunications systems and commercially-developed information security systems are included in the systems referenced under this act.

As a result, in most cases, government agencies can use security-related features of Communication Manager to secure telecommunications data. Communication Manager security features can also help prevent unauthorized access to the customer's network, in general.

Features related to system security and documented in more detail in other sections of this document are listed in Table 48: Communication Manager security and compliance of FISMA on page 196.

Table 48: Communication Manager security and compliance of FISMA

Feature	How related to FISMA	Where documented
Encryption	Transmitted data is protected from packet-sniffing and eavesdropping and other unauthorized access.	See: ● Avaya's encryption overview on page 43
System access control	Access to data is protected from unauthorized personnel	See: ● Managing administrative accounts on page 110
Authentication	Access to the system is restricted by login/password.	See: ● Administering authentication passwords on page 111
Logging	Security-related events are logged	See: ● Configuring SNMP and syslog on page 116 ● Reading and interpreting the security logs on page 170
		1 of 2

Feature	How related to FISMA	Where documented
Firewall	Access to Communication Manager network is protected	See: ● Firewall protection on page 24
Backup of data	Data saved on backup media or backup server. Protected by encryption and key	See ● Secure backups of Communication Manager data and translations on page 204
Toll fraud prevention	Unauthorized use of long-distance is prevented	See ● Limiting long distance access on page 115
		2 of 2

Considerations for customers who want to comply with ISO 17799

ISO 17799 of the International Standards Organization, "Information technology - Security techniques - Code of practice for information security management," is an internationally-accepted standard of good practice for information security. ISO 17799 suggests a well structured set of controls to address information security risks, covering confidentiality, integrity and availability aspects. None of the suggested controls is mandatory, however, an organization wishing to be in compliance should show a security strategy that explains the decision not to implement key controls.

See Table 49: Communication Manager security and compliance of ISO 17799 on page 197 on how ISO 17799 addresses the different categories of data security management.

Table 49: Communication Manager security and compliance of ISO 17799

ISO 17799 Security Guidelines	Communication Manager features and processes
Ensure that applications process information correctly	
● Use validation checks to control processing	Use the System Log and Maintenance Alarm and Event logs. See: ● Configuring SNMP and syslog on page 116 ● Reading and interpreting the security logs on page 170
	1 of 4

ISO 17799 Security Guidelines	Communication Manager features and processes
● Validate data input into your applications	Communication Manager can track administration and notify the administrator when changes are made. Use the System Log, and the Maintenance Alarm and Event logs. See: ● Configuring SNMP and syslog on page 116 ● Reading and interpreting the security logs on page 170 ● *Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers (03-300432)* ● *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers (03-300431)*
● Protect message integrity and authenticity	Use digital certificates when transmitting data to ensure authorization. Restrict access to the system with logins, passwords, and authentication keys. See: ● Chain of trust on page 78 ● Administering authentication passwords on page 111
● Validate your applications' output data	Use audits and status reports to verify output. See: ● *Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers (03-300432)* ● *Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers (03-300431)*
● Use cryptographic controls to protect your information	Encrypt data to protect data from packet-sniffing and eavesdropping. See: ● Avaya's encryption overview on page 43 ● Secure updates of Avaya software and firmware on page 205
	2 of 4

ISO 17799 Security Guidelines	Communication Manager features and processes
Protect and control your organization's system files	
● Control the installation of operational software	Communication Manager requires the appropriate access control in order to install software. In addition, a digital certificate from the software ensures the software is allowed to be installed on the server. See ● Security problems addressed by digital certificates on page 31 ● Secure updates of Avaya software and firmware on page 205
● Control the use of system data for testing	Avaya uses internal ISO-certified testing processes for software.
● Control access to program source code	Communication Manager source code is not accessible outside of Avaya. The Red Hat Linux operating system is also restricted. See ● Why Avaya chose the Linux operating system for Communication Manager on page 23
Control development and support processes	
● Establish formal change control procedures	Avaya uses internal ISO-certified change control processes for software. For security-related updates, Avaya uses a change policy as documented in How Avaya delivers security updates on page 184.
● Review applications after operating system changes	Avaya uses internal ISO-certified test procedures after operating system changes. See Validating a security update on page 186.
● Restrict changes to software packages	Avaya includes only the Linux software packages it needs for Communication Manager. Communication Manager software is proprietary, and Linux software cannot be changed on an installed system. Standard program binaries are normally installed with write permissions only to the super-user (root) and cannot be modified.
● Prevent information leakage	Communication Manager does not have antivirus, antiworm, or antitrojan software. However, Avaya does not recommend using third-party antivirus software on Communication Manager. For more information, see Planning against viruses and worms and other malicious code on page 27.
	3 of 4

ISO 17799 Security Guidelines	Communication Manager features and processes
● Control outsourced software development	Avaya software, if outsourced, is developed according to Avaya's ISO-certified processes.
Control your technical system vulnerabilities	Communication Manager offers many features and processes to protect the customer's communications network. See: ● Avaya's encryption overview on page 43 ● Managing administrative accounts on page 110 ● Configuring SNMP and syslog on page 116 ● Chain of trust on page 78 ● Avaya Public Key Infrastructure on page 80 ● Configuring SNMP and syslog on page 116 ● Secure backups of Communication Manager data and translations on page 204 ● Secure updates of Avaya software and firmware on page 205
	4 of 4

Considerations for customers who must comply with E911

Note:

This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the act's requirements. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

In 2005 the U.S. Federal Communications Commission issued the order, IP-Enabled Services and E911 Requirements for IP-Enabled Service Providers, First Report and Order and Notice of Proposed Rulemaking. The order required providers of interconnected voice over Internet Protocol (VoIP) service to supply enhanced 911 (E911) capabilities to their customers. However, these acts currently apply only to telephone and IP telephony service providers and *not* to enterprise telephony users. Therefore, the E911 Act does *not* currently apply to Communication Manager.

However, the Occupational Safety and Health Administration (OSHA) might consider failure to implement E-911 as a direct violation of Section 5(a)(1) of the Occupational Safety and Health Act, also known as the General Duty Clause, which requires employers to furnish a workplace which is free from recognized hazards, which may cause, or are likely to cause, death or serious physical harm.

In addition, there are roughly 17 states with current or pending legislation requiring enterprise switches to be able to dial 911 and report the caller's number, associated with a physical location. The customer must check with the regulations of the customer’s state to clarify what state requirements might exist regarding 911 calling for enterprises providing telephone systems for employees.

Communication Manager compliance with 911

Traditional telephony

Communication Manager supports both 911 and E911 requirements. For traditional telephones calling the 911 emergency number, Communication Manager uses its automatic routing table to send the emergency call over an ISDN trunk and include the Calling Party Number for automatic identification by the PSAP. In this way, the PSAP, using its Automatic Location Information (ALI) database, can immediately identify the location of the emergency. Alternatively, Communication Manager can send the call to the Public Safety Answering Point (PSAP) through a Centralized Automatic Message Accounting (CAMA) trunk, which sends Caller Emergency Service Identification (CESID) to the PSAP.

For communications systems supporting geographically dispersed locations for which there are different PSAPs, Communication Manager supports a separate CAMA, ISDN, or central office trunk for each location so that the 911 call and location identification is sent to the correct PSAP.

IP telephony

For IP telephones, SIP-enabled telephones, or Softphone, all of which do not have a physical connection to the Communication Manager server or gateways but access the communications system over the LAN, Communication Manager uses the subnetwork to identify the location of the telephone. Communication Manager then converts this location into an Emergency Location Information Number (ELIN) and passes the ELIN on to the PSAP. For Softphone only, Communication Manager also allows the user to enter a phone number which the PSAP can then use to identify the user’s location during an emergency call. For some types of E911 locating capabilities, the Cielo E-911 Manager from RedSky Technologies, Inc. offers more precise location capabilities. Contact RedSky for more information about how that product interacts with Communication Manager E911 capabilities. The Web site for RedSky Technologies, Inc. is http://www.redskytech.com. For more information on Communication Manager 911 and E911 capabilities, see *Avaya Aura™ Communication Manager Feature Description and Implementation (555-245-205)*.

Considerations for non-US customers who must comply with regulations

Any specific country might have unique regulations that raise compliance issues for Communication Manager. For example, countries such as Switzerland and Liechtenstein have Banking Secrecy laws that require a financial organization to inform a customer when the customer's identity has been revealed or that information that might reveal the customer's identity has been released. Such revelations can have negative affect on a bank's business. Therefore, a bank's communications services must be secure to prevent unauthorized access to data such as names, telephone numbers, account codes, and so on. To that end, Communication Manager, through its authentication processes, access control, and encryption methods, can protect call detail records, as well as the calls to customers. In this way, Communication Manager can help a customer comply with banking secrecy laws and protect the integrity of its business. Communication Manager also offers these security features to protect administered data that might reveal a customer's identity, as might be the case, for example, if a customer's IP address or phone number is contained within the firewall rules established for Communication Manager.

Basel II

Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework is a comprehensive set of banking standards compiled by the Basel Committee on Banking Supervision. The national banking overseers in many European countries seek to implement country-specific laws and procedures to meet the Basel II standards. To measure risk levels for a banking standards, Basel II mandates tracking of loss event data, which includes financial systems hacking, theft of data, and impersonation. To this end, Communication Manager systems offer a number of security features, such as those described in the previous paragraph, to minimize loss event data, and therefore, risk level measurements.

For any country in which Communication Manager is sold, there might be a need to inform customers about Communication Manager support for governmental regulations. In this case, the sales engineer or account executive should engage an Avaya legal officer, security specialist, or a compliance specialist to determine the specific ways in which Communication Manager might help the customer comply with regulations.

Common Criteria

The Common Criteria for Information Technology Security Evaluation (CC) and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Agreement (CCRA), which ensures that:

- Products' security properties are evaluated by competent and independent licensed laboratories to determine their assurance.

- Supporting documents that are used within the Common Criteria certification process define how the criteria and evaluation methods are applied when certifying specific technologies.

- The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation.

- These certificates are recognized by all the signatories of the CCRA.

- Avaya has received the Common Criteria certification for the product Core Telephony.

  The TOE (Target of Evaluation) consists of following components and documents:

  - Avaya Aura^{TM} Communication Manager 5.1 running on Avaya Media Server S8730.
  - Avaya Media Gateway G650 with the three modules listed below:
    - IPSI TN2312BP Firmware 44
    - C-LAN TN799DP Firmware 26
    - Medpro TN2602AP Firmware 41
  - Avaya SES Server 5.1 on the Avaya Media Server S8500C.
  - Following modules of Avaya one-X modules:
    - 9630 for H.323, software version 2.0
    - 9630 for SIP, software version 2.4
  - Avaya Secure Service Gateway (SSG) version 3.1.22 on Avaya Media Server S8500C.

The CC web portal (http://www.commoncriteriaportal.org/index.html) reports the status of the CCRA, the CC and the certification schemes, licensed laboratories, certified products and related information, news, and events.

Secure backups and updates

- Secure backups of Communication Manager data and translations on page 204
- Secure updates of Avaya software and firmware on page 205

Secure backups of Communication Manager data and translations

With Communication Manager, the customer can use some or all of the following methods to keep data secure during backups:

- The use of the Secure Copy Protocol (SCP) to back up and restore data over a LAN connection.
- The use of role-based accounts to authenticate permissions to backup data.
- The use of password-protected accounts over the LAN for the backup of data.

  Note:
  The customer must remember the password used for backups in order to restore the data. The password is not retrievable from Communication Manager.

- The use of a 15- to 256-character pass phrase for encryption of the backup of data.

For more information on backing up data with Communication Manager, see “Secure Backup Procedures” in *Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers (03-300432)*.

Note:
You can backup and restore the G250, G350, G430, and G450 Media Gateways using a single CLI command backup and single CLI command for restore.

For information on backup and restore with Media Gateways, see:

- *Administration for the Avaya G250 and Avaya G350 Media Gateways*, 03-300436, chapter 4 for G250 and G350 Media Gateways.

- *Administration for the Avaya G430 Media Gateway*, 03-603228, chapter 5 for G430 Media Gateways.
- *Administration for the Avaya G450 Media Gateway*, 03-602055, chapter 5 for G450 Media Gateways.

Secure updates of Avaya software and firmware

The ability to install software or firmware on Communication Manager is controlled by role-based access controls. The access permissions of the login and the password associated with the login are validated before the software or firmware can be installed. See “AAA Services” in *Avaya Aura™ Communication Manager Feature Description and Implementation (555-245-205)*.

In addition, upgrade firmware and software for some Avaya products, such as the G250, G350, G430 and G450 Media Gateway, the IG550 Integrated Gateway, and TN circuit packs, is signed according to RSA encryption guidelines. Communication Manager authenticates the software or firmware signature upon attempts at installation. If the authentication or certificate does not match, the installation either fails or, in some cases, a warning appears with an option to continue the installation. See Firmware Download Procedures at ftp://ftp.avaya.com/incoming/Up1cku9/tsoweb/firmware/TNpackFirmwareDownloadInstructions.pdf.

When an Avaya server serves as a software or firmware repository from which the software or firmware is downloaded to other Avaya devices, the server provides a certificate for authentication by the downloading device. For example, Communication Manager server provides HTTPS file service for IP telephones. When IP telephones attempt to download firmware from a Communication Manager server over a TLS session, the server provides a certificate for authentication. See *Downloading Avaya 46xx IP Telephone Software Using Avaya Media Servers* at http://support.avaya.com/elmodocs2/white_papers/TFTP_HTTP_Download_External_060504.pdf.

For Communication Manager, the transfer of files between a repository and Communication Manager server or between Communication Manager and other Avaya devices can be accomplished using the Secure Copy protocol (SCP). SCP ensures that the file transfer is secure. See "Copying the software and firmware files to the server" in Chapter 11 of *Installing and Upgrading the G700 Media Gateway and the S8300 Media Server*, 555-234-100.

Remote monitoring and maintenance

Avaya offers Secure Access and Control (SAC) monitoring and maintenance services. SAC uses both Secure Services Delivery Platform (SSDP) and the Secure Services Gateway (SSG) to provide a secure platform from which remote technicians and Expert Systems^{SM} access products at customer sites. for security audits (for example, perimeter scans, penetration tests) and to update and service equipment firmware and alarms, respectively. Using either IP connectivity or traditional dial-in (modem) access, SAC offers service at two levels:

- **SAC Basic** collects alarms from Avaya Products, including modem based alarms, and sends them to Avaya over a B2B VPN/Frame Relay link. Inbound access to products is controlled by SSDP and the customer's firewall.
- **SAC Premium** builds on SAC Basic by adding inbound gateway functionality to the SSG. The customer uses the SSG to control and monitor Avaya's access to their network and products and to record what product was accessed, by whom, when, and why the product was accessed.

Avaya maintenance technicians have access to customer data needed to perform maintenance on customer products, and only authorized Avaya users are permitted access. SSDP logs the user, time and type of access, as well as the reason for the access using the Trouble Ticket number.

SSDP firewall and wireless access

Avaya uses a firewall/VPN product called Secure Gateway 2000 (formerly a VPNet product) on the B2B link. This IPSec, 3DES VPN firewall interoperates with other VPN firewall vendors' products like Cisco, Nortel, and NetScreen.

The DMZ is firewalled off from the rest of the Avaya network. Additional firewalls and intrusion detection systems are deployed throughout the Avaya network partitioning customer servers from other Avaya users.

Remote laptops and desktops use a VPN client to gain wireless access to the Avaya network. They first must connect to the WEP-protected WLAN, then authenticate on the VPN network, and then on the Avaya LAN network.

Remote technicians first access the Avaya LAN using VPN clients. They then authenticate using SSDP's Single Sign-On technology. Authentication and data streams are all encrypted over the WAN.

Remote password complexity and expiration parameters

Avaya programs systems that require secure access to meet its password security policy which dictates the password length and complexity as well as the period of time during which a password cannot be reused. Password length, uniqueness, and repetition restriction are in line with industry practices and are implemented in each of the platforms and applications. Users whose password is about to expire are first notified by email that their account will be disabled in X number of days unless they change their password. If their password is not changed within X number of days, the account is disabled.

Appendix A: Linux-based servers: Avaya S8300 Server

An S8300 Server is an Intel Celeron-based processor that runs the Linux operating system. It resides in one of the following media gateways: G250, G350, G430, G450, G650, or G700.

Detailed description

S8300 version D

The S8300D Server is supported by Communication Manager Release 5.2 and later.

An S8300 Server (version D) is an Intel Core 2 Duo U5700 processor that runs the Linux operating system. The S8300D Server resides in Slot V1 of a Media Gateway and includes:

- A 80-GB hard disk
- 4 GB DRAM (with one 1 GB DIMM)
- 8 GB Internal Solid State Drive (SSD)
- Three USB ports and a 10/100 Base-T port
  - One USB port supports a readable DVD/CD-ROM drive, which is used for system installations and upgrades.
  - One USB port can be used for a USB modem.
  - Another USB port can be used for a Compact Flash drive.
- One services port
- One internal Compact Flash drive, which is used as the primary reboot device
- Modem support for alarming

Software

In addition to Communication Manager software for applications, the S8300D Server runs the following software:

- A Web server that is used for:
  - Backing up and restoring customer data
  - Viewing current alarms
  - Server maintenance, including busy out, shutdown, and status of an S8300D Server.

  - Security commands to enable and disable the modem
  - Security commands to start and stop the FTP server
  - Security commands to view the software license
  - SNMP access to configure trap destinations and to stop and start the master agent
  - Configuration information about the S8300D Server
  - Upgrade access to the S8300D Server
- Maintenance software
- Linux Red Hat operating system
- Trivial File Transfer Protocol (TFTP) server
- Secure HTTP server for IP phone file downloads
- H.248 Media Gateway Signaling Protocol
- Control messages tunneled over H.323 Signaling Protocol

Configurations

The Avaya S8300D Server has the following basic hardware configurations:

- S8300D Server/G700 Media Gateway configuration
- S8300D Server/G430 Media Gateway configuration
- S8300D Server/G450 Media Gateway configuration
- S8300D Server/G350 Media Gateway configuration
- S8300D Server/G250 Media Gateway configuration

An Avaya S8300D Server with a Media Gateway and the gateway’s media modules converge voice and data into one infrastructure. The S8300D Server is an Intel Celeron-based processor that resides in the media gateway. The server has the same dimensions and shape as a media module.

In addition, an S8300D Server can serve as a survivable remote server (Local Survivable Server). See S8300D Server in a Survivable Remote Server configuration on page 217.

Note:
The S8300D Server must be version D to operate Communication Manager R6.0 software.

S8300D Server/G700 Media Gateway configuration

The S8300D Server resides in Slot V1 of a G700 Media Gateway.

A G700 Media Gateway, which is architecturally-based on the Avaya C360 switches, contains VoIP resources and modular interface connectivity. The media modules provide analog, digital, T1/E1, BRI, and additional VoIP capabilities.

Figure 27: S8300D Server in a G700 Media Gateway

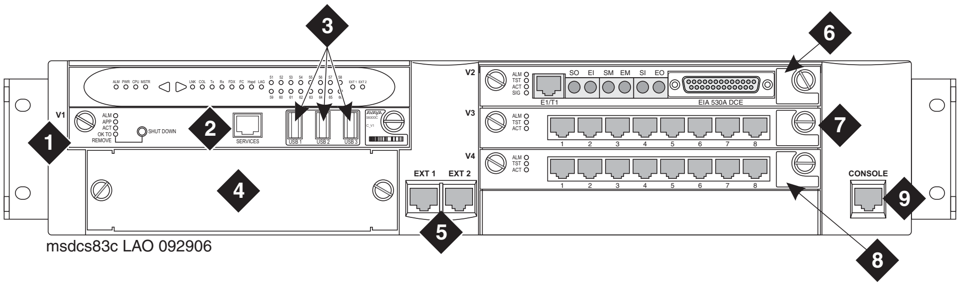


Figure notes:

Number	Description
1.	S8300D Server in Slot V1
2.	Services port
3.	USB ports
4.	Slot
5.	Dual 10/100 Base-T Ethernet switch ports
6.	Media module, Slot V2
7.	Media module, Slot V3
8.	Media module, Slot V4
9.	Console connection for on-site administration

An S8300D Server with a G700 Media Gateway (Figure 27) has the following components:

- Survivability on page 217
- Avaya G700 Media Gateway, which can include:
  - Media modules
  - X330 WAN Access routing module
- S8300D Server in a Survivable Remote Server configuration on page 217
- System Management

For more detail on the S8300D Server, see Survivability on page 217.

S8300D Server/G450 Media Gateway configuration

The G450 Media Gateway features a VoIP engine, an optional WAN router, and Ethernet LAN connectivity. It also provides full support for Avaya IP and digital telephones, as well as analog devices such as modems, fax machines, and telephones. The media modules in a G450 Media Gateway provide analog, digital, T1/E1, BRI, and additional VoIP capabilities.

The G450 supports the S8300D from version S8300B onward. The S8300D runs Communication Manager to provide call control services to the G450. The G450 is compatible with Communication Manager starting with version 5.0.

The S8300D server resides in slot V1. See G450 physical description for the configuration of an S8300D Server in a G450 Media Gateway.

S8300D Server/G430 Media Gateway configuration

The G430 Media Gateway features a VoIP engine, an optional WAN router, and Ethernet LAN connectivity. The G430 provides full support for Avaya IP and digital telephones, as well as analog devices such as modems, fax machines, and telephones.

The G430 supports the S8300D from version S8300C onwards. The S8300D runs Communication Manager (CM) to provide call control services to the G430. The G430 is compatible with Avaya CM from version 5.2.

The S8300D server resides in slot V1. See G430 physical desciption for the configuration of an S8300D Server in a G430 Media Gateway.

S8300D Server/G350 Media Gateway configuration

The G350 Media Gateway features a VoIP engine and WAN router and provides full support for legacy digital and analog telephones. Like the G700 Media Gateway, the media modules in a G350 Media Gateway provide analog, digital, T1/E1, BRI, and additional VoIP capabilities. The following figure shows an S8300D Server and media modules in a G350 Media Gateway.

Figure 28: S8300D Server in a G350 Media Gateway

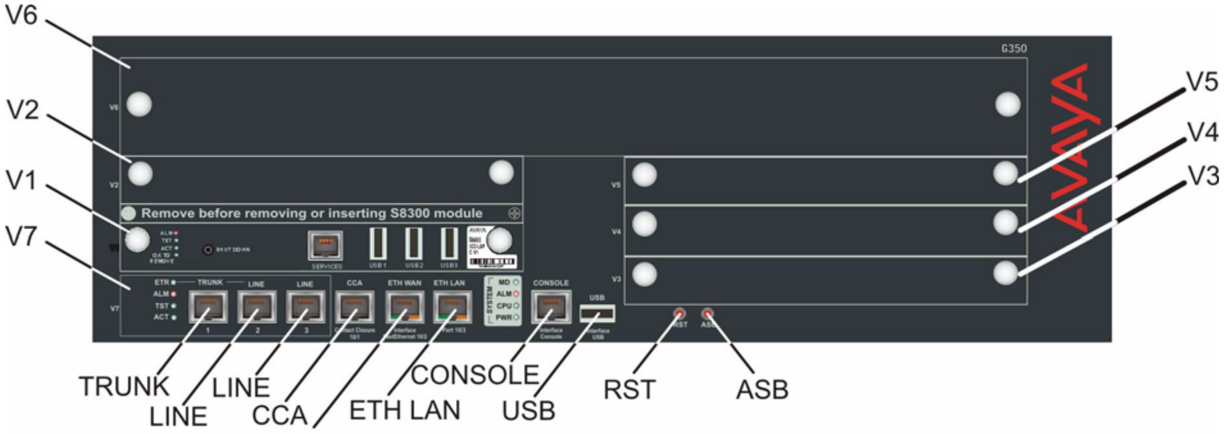


Figure notes:

Port	Description
TRK	An analog trunk port. Part of an integrated analog media module.
LINE 1, LINE 2	Analog telephone ports of the integrated analog media module. An analog relay between TRK and LINE 1 provides Emergency Transfer Relay (ETR) feature.
CCA	RJ-45 port for ACS (308) contact closure adjunct box.
WAN 1	RJ-45 10/100 Base TX Ethernet port.
LAN 1	RJ-45 Ethernet LAN switch port.
CON	Console port for direct connection of CLI console. RJ-45s connector.
USB	USB port for remote access modem.
RST	Reset button. Resets chassis configuration.
ASB	Alternate Software Bank button. Reboots the G350 with the software image in the alternate bank.

An S8300D Server and a G350 Media Gateway configuration has the following components:

- Survivability on page 217
- Avaya G350 Media Gateway, which includes Related hardware
- Communication Manager
- System Management

For more detail on the S8300D Server, see Survivability on page 217.

S8300D Server/G250 Media Gateway configuration

The G250 Media Gateway features a VoIP engine, WAN router, and Power over Ethernet switch. The G250 Media Gateway is available in four models — analog, BRI, DCP, and DS-1. The G250 Media Gateway supports analog and IP telephones. The G250 Media Gateway has built-in media modules. The G250 Media Gateway has two slots available for optional modules — slot V1 houses an optional S8300D Server and slot V2 houses one of two optional WAN media modules.

The following figure shows an S8300D Server in a G250 Media Gateway (analog version).

Figure 29: S8300D Server in a G250 Media Gateway (analog version)

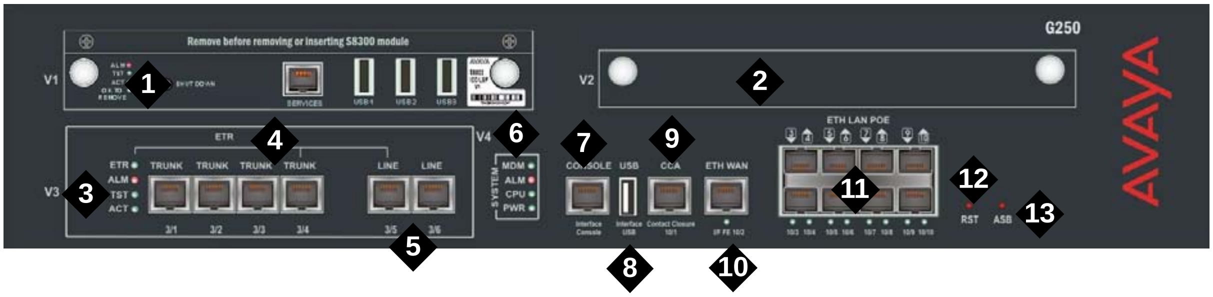


Figure notes:

1. V1 — S8300D/Survivable Remote Server Slot
2. V2 — WAN Media Module Slot
3. Analog port LEDs
4. Analog trunks
5. Analog line ports
6. System LEDs
7. Console port
8. USB port
9. Contact Closure (CCA) port
10. Ethernet WAN (ETH WAN) port
11. PoE LAN (ETH LAN PoE) ports
12. Reset (RST) button
13. Alternate Software Bank (ASB) button

An S8300D Server and a G250 Media Gateway configuration has the following components:

- Survivability on page 217
- Media gateways and integrated gateways
- Communication Manager
- System Management

For more detail on the S8300D Server, see Survivability on page 217.

Components

For a list of S8300D components used in each S8300D configuration, see Configurations on page 210.

UPS or power backup

For the S8300D Server, any of the available UPS units can instantly supply power during a power outage.

RAM disk

RAM disk is a portion of memory used as a disk partition. In the event of a hard disk failure, the S8300D Server uses only RAM disk to provide call processing for up to 72 hours. Administration and backups are prohibited. Also, Communication Manager messaging (CMM) is unavailable when operating in RAM disk mode so secondary call coverage points for users should be administered, even with RAM disk enabled.

Note:
The S8300D server does not support RAM Disk.

Related hardware and adjuncts

Communication Manager Messaging

Note:
The IA770 INTUITY AUDIX messaging is called Communication Manager messaging, starting with Communication Manager R5.2 and later releases.

Communication Manager messaging (CMM) is an optional voice mail system used with an S8300D Server. Communication Manager messaging is a software-only version of messaging that uses a QSIG-MWI H.323 virtual trunk for communication between the Communication Manager and Communication Manager messaging software. This version is available on the G700, G450, G430, G350, and G250 Media Gateway configurations. Without the need for additional hardware, Communication Manager messaging software processes touchtones, converts messages to the G.711 format, and converts text to speech.

Note:
The Communication Manager messaging application is included with Communication Manager R6.0 with many of the Communication Manager templates.

The Communication Manager messaging system can be a solution for one location in a stand-alone S8300D configuration. The system can also be networked with other voice mail systems using TCP/IP and Avaya Message Networking.

An Communication Manager messaging uses many resources of the S8300D Server and the media gateway where it resides. The following list outlines the S8300's shared resources used by the Communication Manager messaging system:

- Hardware for data storage and retrieval
- TFTP server for:
  - Downloading and updating the license file for feature activation
  - Backing up and restoring data over a LAN or a WAN, including translations and messages
  - Updating and upgrading software
- IP address for administration access
- General Alarm Manager for alarm display
- Web interface to start and stop the system

The Communication Manager messaging system also shares the same switch-tone parameters established for the S8300D Server. The S8300D Server handles switch tones on behalf of the Communication Manager messaging system and passes on the control information to the Communication Manager messaging system using QSIG signaling.

Call center

An S8300D Server provides an excellent solution for a small call center. The S8300D also offers the following call-center capabilities:

- A maximum of 16 ASAI links
- Announcement software

With large announcement storage including optional compact flash, large voice trunk capacity, and 16 announcement ports for announcement record and playback, the G430 supports call center features.

Printers

The S8300D Server is connected to the customer's LAN. Therefore, you can send print requests to any printer within the LAN and IP region of the S8300D Server.

A system printer is supported when a terminal server is used. In this case, the printer is connected to an adjunct PC such as a CDR system, CMS, or Call Accounting System.

A journal printer is supported when a terminal server is used.

Survivability

S8300D Server in a Survivable Remote Server configuration

An S8300D Server in a Survivable Remote Server (Local Survivable Processor) configuration uses the S8300D hardware component and a software license to activate a standby feature. This software allows the Survivable Remote Server with a Media Gateway to be a survivable call-processing server for remote locations and branch locations.

The branch locations can have the following servers as their primary controller:

- S8300D
- S8510
- S8800

An S8300D Server and the Survivable Remote Server cannot reside in the same Media Gateway.

If for any reason communication between a Media Gateway and its primary controller stops, a Survivable Remote Server activates. This "fail-over" from the primary controller to the Survivable Remote Server is an automatic process without human intervention. The Survivable Remote Server assumes control of any IP telephone provided that telephone has the Survivable Remote Server in its list of controllers.

The Survivable Remote Server can continue to support calls as the primary controller for 30 days. The Survivable Remote Server is in "license-error" mode when it is supporting calls. After 30 days in license-error mode, the Survivable Remote Server administration is blocked and display telephones show **License Error** in their display windows. However, even after 30 days, telephone operations can continue.

Automatic fallback to primary controller

Based on administration of Communication Manager, the G250/G350/G430/G450/G700 Survivable Remote Server can return control of the G250/G350/G430/G450/G700 Media Gateway to the primary controller (server) automatically when the connection is restored between the media gateway and the primary controller. By returning control of the media gateways to the primary controller automatically, Communication Manager software easily and quickly eliminates the fragmentation between remote gateways in the network created by LAN/WAN communication failures with the primary controller.

The Media Gateway preserves stable calls when control changes from the Survivable Remote Server to the primary controller. Stable calls are calls that are carrying active two-way or multi-party conversations. Other calls such as those that are on hold are not preserved.

Note:
The fall-back from the Survivable Remote Server to the primary controller may also be manual using a reset on the Survivable Remote Server. This reset breaks the communication between the Survivable Remote Server and each registered endpoint. This break causes the endpoints to register with the primary controller. However, most active calls are preserved.

Number of Survivable Remote Servers supported

The number of Survivable Remote Servers that a configuration can support depends on the controlling server. An S8510 and S8800 Server can support up to 250 Survivable Remote Servers. An S8300D Server can support up to 50 Survivable Remote Servers.

Translations

An automatic process copies translation changes when customers make changes on the primary controller to each Survivable Remote Server.

Hardware Requirement

The hardware for the S8300D Server as primary controller is identical to the hardware for the S8300D Server as Survivable Remote Server. The difference between the two configurations is entirely in software.

IP addressing of the primary controller, the Survivable Remote Server, and IP telephones

A Survivable Remote Server is administered with a different IP address than the IP address of the primary controller. In addition, IP telephones obtain their own IP address from a DHCP server. The DHCP server also sends a list of controllers, Survivable Remote Servers, and their associated IP addresses. The IP telephone then registers with the controller corresponding to the first IP address in this list. When connectivity is lost between the controller and the endpoint, the endpoint registers with the second IP address in the list, and so on. This list can be administered for telephones on the DHCP server.

High-level capacities

The S8300D Server supports:

- 900 ports by a combination of trunks and stations
  - 450 IP stations, 450 non-IP stations, or a combination of 450 IP and non-IP stations
  - 450 trunks

- 50 G250/G350/G430/G450/G650/G700 Media Gateways

Table 50: High-level capabilities

Capability	S8300D Server
Call processing feature set	Communication Manager 3.0
Maximum number of stations	450 (IP or TDM)
Maximum number of trunks	450
Reliability options	Single server
Port-network connectivity	Not applicable
Supported media gateways	G250, G350, G430, G450, G650, G700
Maximum number of supported gateways	50 (supported by one S8300D Server)
Survivability options	G250, G350, G430, G450, G650, and G700 with S8300D Survivable Remote Server
Number of Survivable Remote Servers in one configuration	Maximum of 50 when supported by an S8300D. Maximum of 250 when supported by an S8510 or S8800 Servers
Port networks	Not applicable

For more detailed system capacity information, see the *Avaya Aura™ Communication Manager System Capacities Table,* 03-300511.

Appendix B: Linux-based servers: Avaya S8510 Server

The Avaya S8510 Server is a single server. The S8510 Server run the Linux operating System, and feature Communication Manager. The S8510 Server can support Internet Protocol (IP), Session Initiation Protocol (SIP), and traditional endpoints. This tri-level support enables new technology and eases migration from legacy Avaya systems. The S8510 Server is a perfect solution for mid-sized customers, with growth of up to 3200 ports.

Detailed description

An S8510 Server configuration includes the following:

- S8510 Server on page 222
- Media gateways for main locations, which individually or as stacks connect to port networks through Avaya G650 Media Gateway, which is always sold with new systems.

  Note:

  If used as a survivable remote server, the Avaya G700 Media Gateway, the Avaya G430 Media Gateway, the Avaya G450 Media Gateway, the Avaya G350 Media Gateway, and the Media gateways and integrated gateways are supported through the processor ethernet interface.Media Gateway types cannot be mixed within the same port network (PN).

- TN2312BP IP server interface, which provides control signaling between the server and the port networks (PNs). At least one PN in a fiber-connected configuration must contain a TN2312BP circuit pack. In an IP-connect configuration, each PN must contain one TN2312BP circuit pack.
- TN2302AP IP media processor or TN2602AP IP Media Resource 320, which provides TDM-to-IP conversions of audio signals. At least one of these circuit packs is required in each IP-connected PN.
- Communication Manager
- System Management

The S8510 Server supports secure HTTP server for IP phone file downloads.

The S8510 Server supports IP port network connections: single control network (IP-PNC)

S8510 Server

The Avaya S8510 Server uses the Linux operating system and supports several Avaya software applications. It is generally used in single server mode, but in some circumstances can be duplexed. The Avaya S8510 server is targeted for the mid-sized customer.

Functionally, the S8510 is extensively tailored around the S8510 Server. The major architectural and functional differences between the S8510 and the S8500C are:

- The S8510 hardware platform is a Dell multi-core CPU platform.
- The S8510 does not support the RAMDISK feature but instead supports the hardware version of RAID (Redundant Array of Independent Disks) Level 1 industry standard feature with Dual Hard Disk Drives (HDD).

The S8510 server comes equipped with the Augmentix A+SAMP^{TM} card for remote maintenance and serviceability of the server, and the Dual NIc card. The S8510 system comes equipped with one (1) modem off of the A+SAMP^{TM} USB port that will be shared between the HOST server and the A+SAMP^{TM} card for remote maintenance, administration, and alarming purposes.

The S8510 server hardware system comes equipped with the hardware version of the RAID Level 1 feature. This feature employs the disk mirroring method which creates a set of data on two or more disks. A general RAID 1 mirrored pair contains two disks which increases the reliability of the system. Each of the disks is independent of each other and contains a complete copy of the data.

The default S8510 server configuration has a single Power Supply. However, the S8510 server supports the redundant Power Supply configuration, and a customer can choose to order an extra Power Supply.

See Figure 30: S8510 Server (front) on page 223 and Figure 31: S8510 Server (back) on page 224 for examples of the front and back of the S8510 Server.

Figure 30: S8510 Server (front)

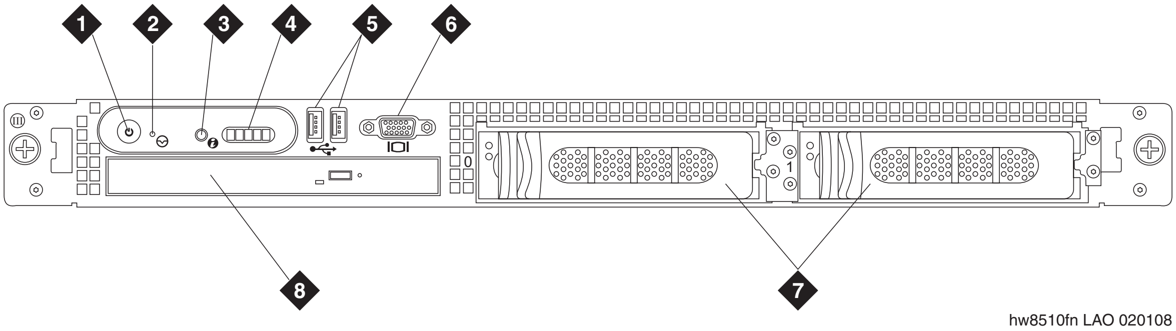
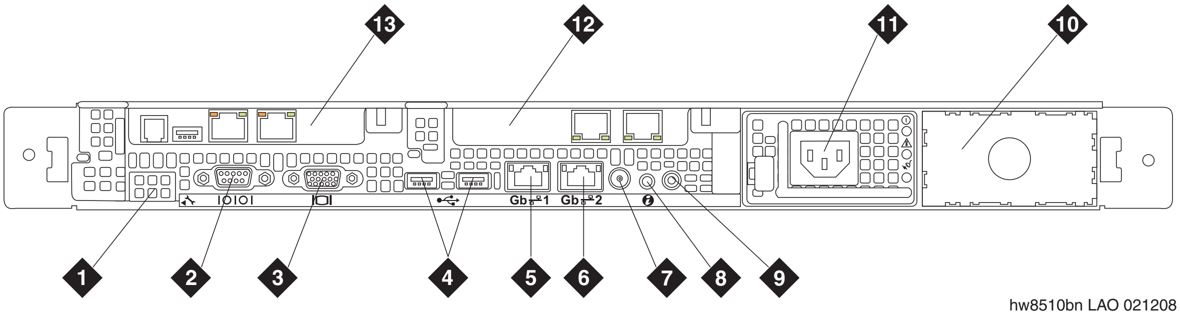


Figure notes:

1. **Power-on LED**
2. **NMI button (not used)**
3. System ID button
4. LCD display
5. **USB ports**
6. **Video connector (not used)**
7. Hard disk drives
8. **Optical DVD/CD drive**

Figure 31: S8510 Server (back)



hw8510bn LAO 021208

Figure notes:

1. **Remote access controller (not used)**
2. **Serial connector (not used)**
3. Video connector (not used)
4. USB ports (not used)
5. **GB-1 (Eth0)**
6. **Services port - GB-2 (Eth1)**
7. Services status indicator connector
8. **System ID button**
9. **System Status LED**
10. Bay for optional redundant power supply
11. **Power supply**
12. **Dual NIC**
13. **Remote maintenance board (SAMP)**

S8510 LED Indicators

Figure 32 shows the drive status/activity LEDs.

Figure 33 show the status LEDs on the back of the S8510.

Table 51 describes the LED indicator conditions for power, power supply, AC line status, and drive status.

Figure 32: S8510 Server (drive status/activity)

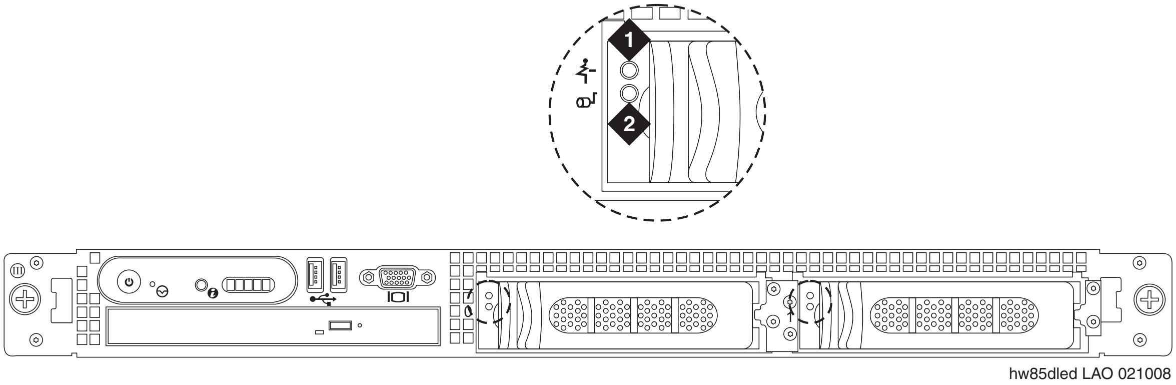
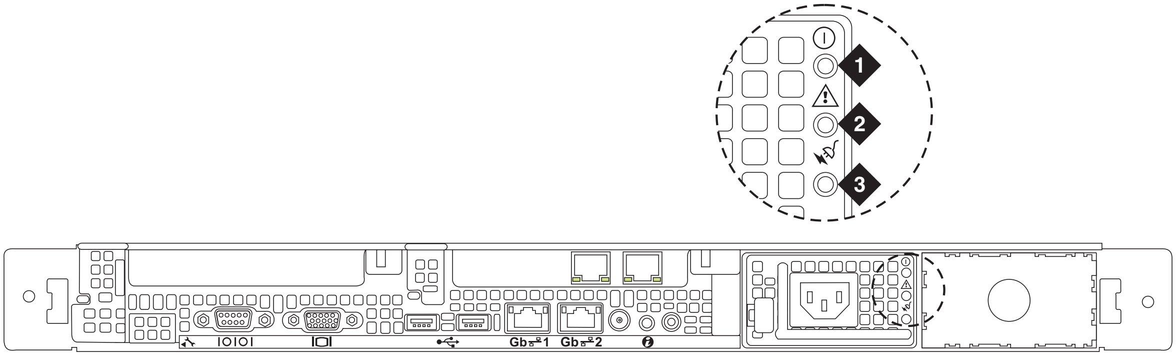


Figure notes:

1. Drive status
2. Drive activity

Figure 33: S8510 Power Supply/AC Line LEDs



hw85pled LAO 021008

Figure notes:

1. **Power supply status**
2. **Power supply fault**
3. **AC line status**

Table 51: S8510 LED indicator conditions *1 of 2*

LED	Indicator/Pattern	Function/Condition
Power Button	On	System has power and is operational
	Off	System has no power
Power Supply Status	Green	Power supply is operational
Power Supply Fault	Amber	There is a problem with the power supply
AC line status	Green	Power supply is connected to a valid AC power source
Drive status	Off	Drive ready for insertion or removal
	Steady green	Drive online
	Blinks green, amber, off	Drive predicted failure

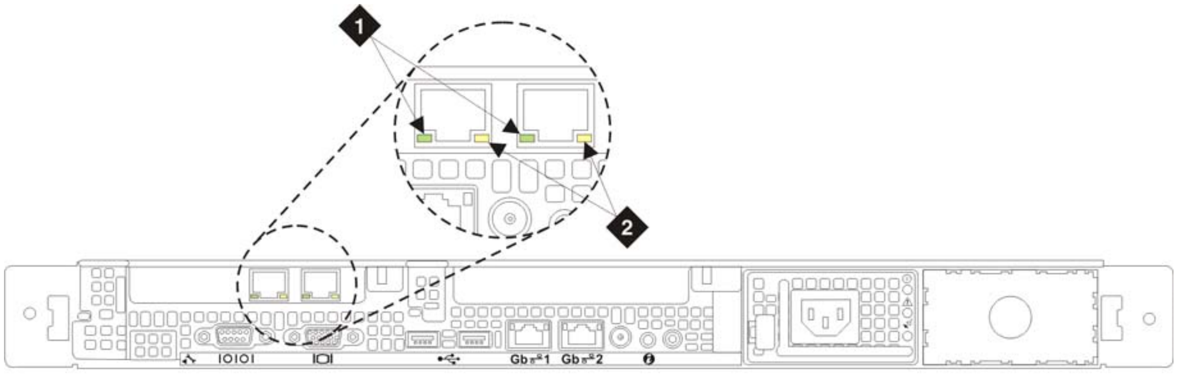
Table 51: S8510 LED indicator conditions *2 of 2*

LED	Indicator/Pattern	Function/Condition
	Blinks amber 4 times per second	Drive failed
	Blinks green 2 times per second	Identify drive/preparing for removal
	Blinks green slowly	Drive rebuilding
	Blinks green 3 seconds, amber 3 seconds, off 6 seconds	Rebuild aborted
Drive activity	Blinks green	Drive has activity

NIC Indicator Codes

Each NIC on the back panel has an indicator which provides information on network activity and link status. Figure 34 describes the NIC indicator codes.

Figure 34: NIC Indicator Codes



hw85nicl LAO 050108

1	Network activity (TX/RX)
2	Connection rate ● Off: 10BaseT active link ● Green: 100BaseT active link ● Amber: 1000BaseT active link

Configurations

S8510 Server Components

The S8510 comes with the following components:

- One Quad Core Intel® Xeon® E5410 Processor 5000 Sequence.
- A minimum of 2 GB (2 x 1 GB) of 667 MHz (when available), fully buffered DIMMs (FBD), upgradable to a maximum of 32 GB by installing combinations of 1-GB, 2-GB, or 4-GB memory modules in the eight memory module sockets on the system board.

Servers dedicated to Release 6.0 Communication Manager must have 8 GB of physical memory.

The system also features redundant memory, which provides memory sparing or memory mirroring. Either feature is available if eight identical memory modules are installed.

- Support for two 3.5-inch, internal hot-pluggable SATA (7200 rpm) hard drives.
- An optional slimline DVD-ROM/ CD-RW drive.
- One hot-pluggable, 670-W power supply with an option of installing a second power supply in a 1 + 1 redundant (optional) configuration.
- Four fan modules, each comprises two dual-rotor fans, for a total of eight cooling fans.

The system board includes the following features:

- One dual network interface card (NIC)
- Two integrated gigabit Ethernet NICs capable of supporting 10-Mbps, 100-Mbps, and 1000-Mbps data rates.
- Four USB 2.0-compliant connectors. Two on the front support an optional mouse and keyboard. The two on the back are not used in the Communication Manager Release 5.1 time frame.
- An integrated VGA-compatible video subsystem with an ATI ES1000, 33-MHz PCI video controller.
- Back-panel connectors include serial, video, two USB connectors, and two NIC connectors.
- Front-panel connectors include a video and two USB connectors.
- Front-panel 1x5 LCD for system ID and error messaging.

RAID

The S8510 supports the hardware version of RAID (Redundant Array of Independent Disks) Level 1 industry standard feature with Dual Hard Disk Drives (HDD). A general RAID 5 mirrored pair contains two disks which increases the reliability of the system.

Each of the disks is independent of each other and contains a complete copy of the data. The primary HDD is mirrored onto the secondary HDD. If either drive fails, the other continues to function without service interruption. If both disks fail, the server is out-of-service.

Replacement of a failed HDD requires no service interruption.

⚠ **CAUTION:**
The firmware associates HDDs with the server. HDDs can be moved as a pair to another server, but in order to do this, you must import the other server's configuration in the RAID-BIOS. This must be done at boot time on a keyboard and a monitor, which have to be connected directly to the server.

The **`raid_status`** bash command displays the server RAID controller status.

There is a new web interface *RAID Status* option under **Diagnostics** on the Main. *RAID HDD Status* is displayed as part of the *Server->Status Summary*.

RAID HDD Status is displayed as part of the **`server`** bash command.

Value	Description
1	1 HDD operational
2	2 HDD operational
-1	1 or 2 failed HDD; error in acquiring HDD information

S8510 Server Specifications

The following table outlines the specifications of the S8510 Server.

Type	Description
Processor	
Processor type	1 Quad-core Intel Xeon E5410 processor 5000 sequence
Expansion bus	
Bus type	PCIe

Type	Description
Memory	
Architecture	PC2-4100 667 MHz fully buffered DIMMs with ECC protection
Memory module sockets	8 240-pin
Memory module capacities	1 GB, 2 GB, 4 GB
Min/Max RAM	1GB/32 GB
Drives	
SATA hard drives	2 3.5 in., internal hot-pluggable with backplane support
Optical drive	1 DVD-ROM/CD-RW combination
Connectors (front)	
USB	2 4-pin, USB 2.0 compliant
Video	15-pin VGA
Connectors (back)	
NIC	2 RJ-45
Serial	9-pin, DTE, 16550-compatible
USB	2 4-pin, USB 2.0 compliant
Video	15-pin VGA
AC power supply	
Wattage	670 W
Voltage	90-264 VAC, autoranging, 47-63 Hz, 10.0 A (at 90 VAC)
Heat dissipation	2697 BTU/h (maximum)
Maximum inrush current	Under typical line conditions and over the entire system ambient operating range, the inrush current may reach 55 A per power supply for 10 ms or less.
System battery	CR 2032 3.0-V lithium ion coin cell
Dimensions (HxWxD/Us)	1.7 x 19 x 30 in. (4.3 x 48.3 x 7.26 cm)/1 U
Weight	39 lb (17.7 kg)

⚠ **DANGER:**
The Avaya S8510 Server contains lithium batteries. These batteries are not customer field replaceable parts. Do not disassemble. Batteries may pose a hazard if mishandled.

Environmental requirements

Type	Description
Temperature	
Operating	10° to 35°C (50° to 95°F)
Storage	–40° to 65°C (–40° to 149°F)
Relative humidity	
Operating	8% to 85% (non-condensing) with a maximum humidity gradation of 10% per hour
Storage	5% to 95% (non-condensing)
Maximum vibration	
Operating	0.25 G at 3–200 Hz for 15 min
Storage	0.5 G at 3–200 Hz for 15 min
Maximum shock	
Operating	One shock pulse in the positive z axis (one pulse on each side of the system) of 41 G for up to 2 ms
Storage	Six consecutively executed shock pulses in the positive and negative x, y, and z axes (one pulse on each side of the system) of 71 G for up to 2 ms
Altitude	
Operating	–16 to 3048 m (–50 to 10,000 ft)
Storage	–16 to 10,600 m (–50 to 35,000 ft)

Related hardware

Table 52: S8510 Server Hardware Specifications

Specification	S8510 Server
Processor	2 GHz Quad Core
SDRAM Memory	8GB

Table 52: S8510 Server Hardware Specifications

Specification	S8510 Server
Hard Drives	250GB SATA RAID Level 1 Duplicated Redundant disk drive
On-Board NICs	Dual Gigabit Ethernet 10/100/100
Optical Drive	CD RW/DVD read-only drive
SAMP Remote Maintenance Card	PCI-e slot SAMP Lite Adapter
NIC Card	1 X Dual NIC PCI-e Card (100/1000)
Diagnostic Indicators	LEDs and Alphanumeric Display
Form Factor (HxWxD) Weight	1U High: 1.7" x 19" x 30" 39lb (17.7kg)
Fans	Redundant Fans
Power Supply	Dual (Optional) Redundant Hot Pluggable

Survivability

Note:
This section applies to S8510 Server.

Recovery capability is embedded in the Communication Manager software that resides on the S8510 Server. Thus, the servers can use the following recovery options:

- Servers, port networks, and gateways that S8510 Survivable Core Server supports on page 233
- S8300 Server in a Survivable Remote mode on page 234

S8510 Server as a Survivable Core Server

A Communication Manager configuration may use the S8510 Server as a Survivable Core Server (Enterprise Survivable Server). The Survivable Core Server option provides survivability to a configuration by allowing backup servers to be placed in various locations in the customer's network. An Survivable Core Server assumes call processing control of all or part of the configuration in case the main server, either S8510 or S8800 Server, fails or network connections to the main server fail.

A main server may have many, up to 63, Survivable Core Server available to provide backup service. The placement of the Survivable Core Server or Survivable Core servers in the configuration is typically targeted at ensuring that port networks that are configured in different segments of the customer's LAN/WAN can receive service even when LAN/WAN connections are lost.

Once the communication failure to the main server has been corrected, control of call processing may be returned from the Survivable Core Server to the main server either manually port network by port network or automatically for all port networks at once.

Note:

In the transition of control from the main server to an Survivable Core Server, all calls are dropped while the media gateways carrying the calls reset to connect to the Survivable Core Server.

Servers, port networks, and gateways that S8510 Survivable Core Server supports

The S8510 Server may serve as the Survivable Core Server for either an S8510 or an S8800 main server. If the main server is a S8510 Server, any and all Survivable Core Server in the configuration must also be S8510 Server. The S8510 Server, Survivable Core Server can maintain the duplication when it takes call processing control from the main server. To support duplication, an S8510 Server Survivable Core Server must also contain a dual-NIC card. Note that when the S8510 Server is used as an Survivable Core Server for the S8800 main, the S8510 Server has the same capacities as the S8800 main.

Note:

An Survivable Core Server may support a G250, G350, G430, G450, G650, or G700 Media Gateway through the C-LAN connection of the Survivable Core Server-connected port network.

Requirements to support CSS- and ATM-connected port networks

Each CSS-connected port network that is to receive Survivable Core Server service must also contain a TN2312BP IPSI circuit pack and TN570 Expansion Interface circuit packs with vintage D or higher. Vintage D of the TN570 allows the TN570 to appropriately share control from the server with the IPSI. To be survivable, any CSS-connected port networks must have an IPSI to get service from an Survivable Core Server and a TN2302AP IP Media Processor or a TN2602AP IP Media Resource 320 to have port network connectivity to the other PNs. A PN without an IPSI will lose service when the main server connection fails.

Each ATM-connect port network that is to receive Survivable Core Server service must also contain TN2305 or TN2306 ATM Interface circuit packs with vintage B or higher. Vintage B of the TN2305/2306 allows the TN2305/2306 to appropriately share control by the server with the IPSI. Any ATM-connected port network that does not have an IPSI may still receive service if the port network maintains its connection to the ATM switch and the ATM switch still communicates with one or more IPSI-controlled port networks.

For more information about Survivable Core Server setup, operation, or feature functionality, see *Avaya Aura™ Communication Manager Survivable Options User Guide*, 03-300428.

S8300 Server in a Survivable Remote mode

The S8300 Survivable Remote Server is located in the G700/G450/G430/G350/G250 Media Gateway and provides survivability when the S8510 Server is inaccessible. Each S8510 Server can have up to 250 Survivable Remote Servers. The S8300D Survivable Remote Server can support up to 50 H.248 media gateways. The Survivable Remote Server has a copy of the S8510 Server customer translations.

Power outages

In most cases, an Avaya solution can recover from a power outage or other failure instantly, regardless of the source of the failure. Each PN includes a set of segmented, parallel buses. If one of the paired segments fails, the other bus segment continues to handle communications. The UPS units supply power to the control complex.

S8510 port connections

Use standard CAT5 cables with RJ45 connectors on each end to connect to the various ports. If the S8510 Server has only one port network, connect that port network through the dual NIC. Figure 35: S8510 Server connectivity guide on page 235 shows typical connectivity for the S8510 Server.

Figure 35: S8510 Server connectivity guide

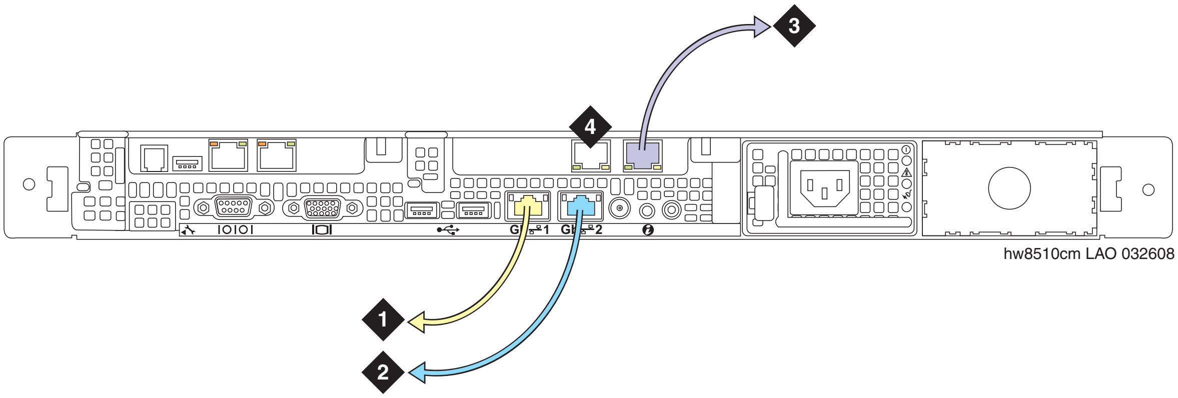


Figure notes:

1. Eth0—To the customer network if the control network is nondedicated. Or, to the control-network Ethernet switch if the control network is dedicated (straight-through CAT5 cable)
2. Eth1—To the Services laptop computer (crossover CAT5 cable)
3. Eth3—to the customer network if the control network is dedicated (straight-through CAT5 cable)
4. Eth4—Not used

S8510 BIOS Upgrade Feature

The **BIOS Upgrade** feature is accessed from the System Management Interface under **Server Upgrades**.

Field Replaceable Units

Field Replaceable Unit
S8510 Server
Hard Disk Drive(s) Redundant Disk Hot Pluggable
Power Supply(s) (Optional) Redundant Power Supply Hot Pluggable

Field Replaceable Unit
Memory
Dual NIC

High-level capacities

Table 53: High-level capabilities

Capability	S8510 Server
Call processing feature set	Communication Manager 3.1. The S8510 Server is supported by Communication Manager releases 5.1 and later.
Reliability options	Single server control and duplicated bearer. Note that Communication Manager 5.1 is the minimum load for the S8510.
Port-network connectivity	IP and direct-connect
Supported port network media gateways	Voice bearer over IP: G650
Maximum number of supported media gateways for branch offices	250 (includes G700, G650, G450, G430, G350, and G250 Media Gateways in any combination)
Maximum locations	64 port networks, plus up to 250 G700/G650/G450/G430/G350/G250 Media Gateways
Survivability options	G250, G350, G430, G450, G650,and G700 Media Gateways with S8300D Survivable Remote Server S8510 Survivable Core Server or Survivable Remote Server
Number of Survivable Remote Servers in one configuration	Maximum of 250 Survivable Remote Servers
Number of Survivable Core Servers in one configuration	Maximum of 63 Survivable Core Servers
Port networks per IPSI	One with IP-connect port networks. Three with direct-connect port networks.

For more detailed system capacity information, see the *Avaya Aura™ Communication Manager System Capacities Table*, 03-300511.

In addition to voice calls, the S8510 Server, through Communication Manager and the use of an appropriate media processor (T2302AP or TN2602AP), supports transport of the following messages:

- Fax, Teletypewriter device (TTY), and modem calls using pass-through mode
- Fax, V.32 modem, and TTY calls using proprietary relay mode

⚠ **SECURITY ALERT:**
Faxes sent to non-Avaya endpoints cannot be encrypted.

Note:
V.32 modem relay is needed primarily for secure SCIP telephones (formerly known as Future Narrowband Digital Terminal (FNBDT) telephones) and STE BRI telephones.

- T.38 Fax over the Internet, including endpoints connected to non-Avaya systems
- 64kbps clear channel transport in support of firmware downloads, BRI secure telephones, and data appliances

Note:
The path between endpoints for modem tone transmissions must use Avaya telecommunications and networking equipment.

See TN2302AP IP media processor or TN2602AP IP Media Resource 320 for more information. See also *Administering Network Connectivity on Avaya Aura™ Communication Manager*, 555-233-504, for more information.

Related Documents

LED Descriptions for Avaya Aura™ Communication Manager Hardware Components, 03-602804

Installing the Avaya S8510 Server Family and Its Components, 03-602918

Server Availability Management Processor: Avaya S8510 Server, 03-602923

Appendix C: Linux-based servers: Avaya S8800 Servers

The Avaya S8800 Server supports several Avaya software applications. The server is available in a 1U model or 2U model and with various hardware components. The server model and specific hardware components in your server depend on the requirements of the software application that will run on the server.

Communication Manager supports the 1U model of the S8800 Server. While installing Communication Manager in simplex mode on the S8800 Server, you only use 1 S8800 Server, whereas, installing Communication Manager in duplex mode requires you to have 2 S8800 Servers.

Avaya S8800 Server Requirements

- Front of server
- Back of server
- Server specifications
- Server components
- Environmental requirements

Front of server

Figure 36: S8800 Server (front view)

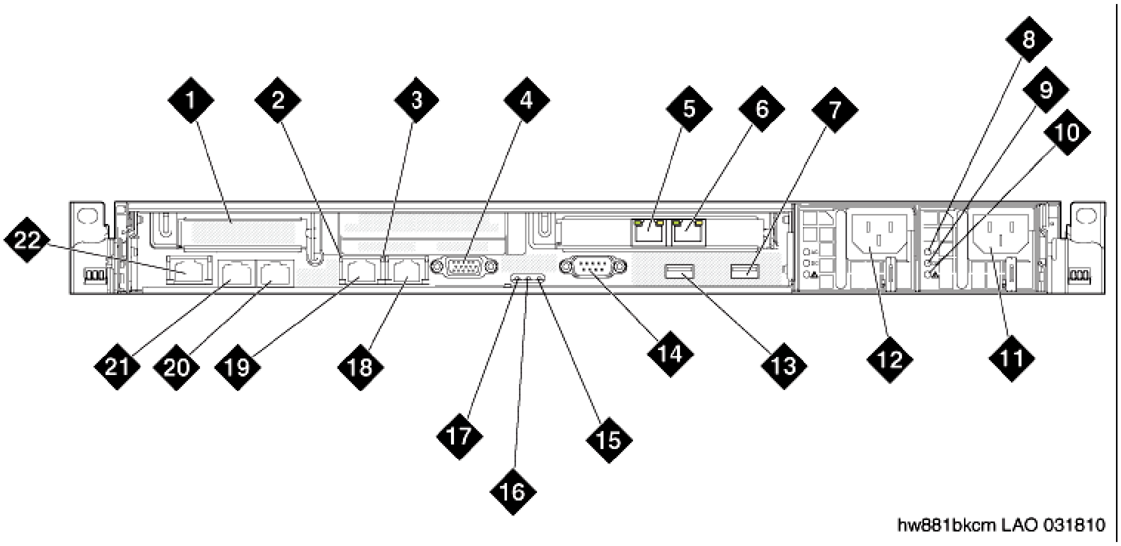


Figure notes:

Number	Description of Device
1.	Hard disk drive activity LED (green)
2.	Hard disk drive status LED (amber)
3.	Drive bay 0
4.	Drive bay 2 (unused for Communication Manager)
5.	Drive bay 4 (unused for Communication Manager)
6.	Power control button and LED
7.	Operator information panel **Note:** The operator information panel is shown in the pushed in position.
8.	Operator information panel release latch
9.	Video connector
10.	USB connector 1
11.	Rack release latch
12.	USB connector 2
13.	DVD eject button
14.	DVD drive activity LED
15.	DVD drive
16.	Drive bay 5 (Unused for Communication Manager)

Number	Description of Device
17.	Drive bay 3 (Unused for Communication Manager)
18.	Drive bay 1
19.	Rack release latch

Back of server

Figure 37: S8800 Server (back view)

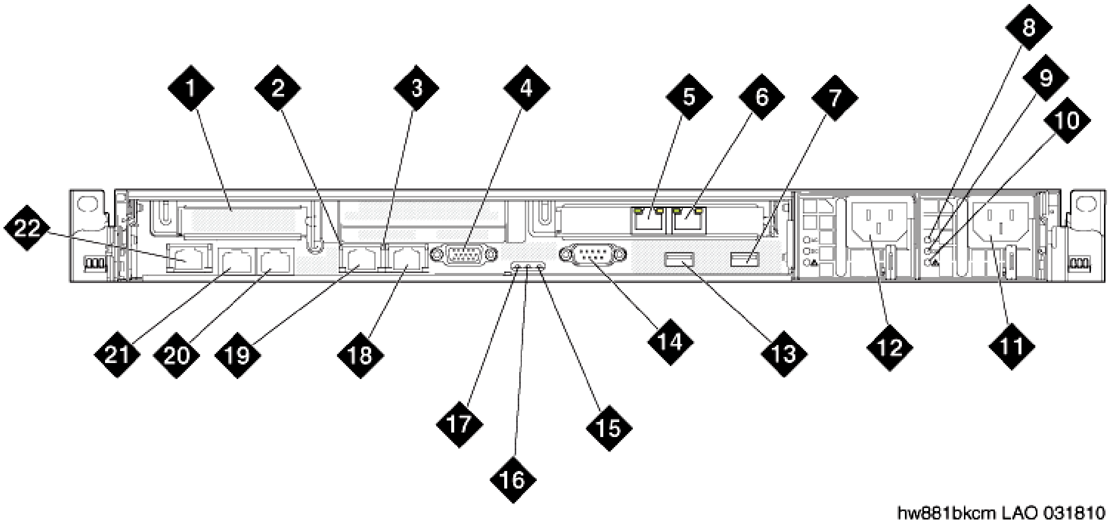


Figure notes:

Number	Description of Device
1.	PCIe slot 1 (unused)
2.	Ethernet activity LED
3.	Ethernet link LED
4.	Video connector
5.	DUAL NIC PCI card (Ethernet connector 6 (eth5)) **Note:** Ethernet connector 6 (eth 5) is unused.
6.	DUAL NIC PCI card (Ethernet connector 5 (eth4) — corporate LAN)
7.	USB connector 4
8.	AC power LED (green)
9.	DC power LED (green)
10.	Power supply error LED (amber)

Number	Description of Device
11.	Power supply 2 (optional redundant power supply)
12.	Power supply 1 (primary power supply)
13.	USB connector 3
14.	Serial connector
15.	System error LED (amber)
16.	System locator LED (blue)
17.	Power LED (green)
18.	Ethernet connector 2 (eth 1) (Services port)
19.	Ethernet connector 1 (eth 0) (Duplication link if configuration is duplicated server)
20.	Daughter card (Ethernet connector 4 (eth 3) - Control Network B)
21.	Daughter card (Ethernet connector 3 (eth 2) - corporate LAN and or Control Network A if configuration is duplicated server)
22.	System management Ethernet connector (IMM)

Note:

Hardware label for Ethernet ports on the server is called Ethernet connectors. Communication Manager software refers to Ethernet ports as eth.

Server specifications

Type	Description
Dimensions	Height: 43 mm (1.69 inches, 1U) Depth: 711 mm (28 inches) Width: 440 mm (17.3 inches)
Weight	Maximum weight: 15.4 kg (34 lb.) when fully configured.
Heat output	Approximate heat output: ● Minimum configuration: 662 Btu per hour (194 watts) ● Maximum configuration: 1400 Btu per hour (400 watts) Heat output varies depending on the number and type of optional features that are installed and the power-management optional features that are in use.

Type	Description
Acoustic noise emissions	Declared sound power, operating: 6.1 bel The sound levels were measured in controlled acoustical environments according to the procedures specified by the American National Standards Institute (ANSI) S12.10 and ISO 7779 and are reported in accordance with ISO 9296. Actual sound-pressure levels in a given location might exceed the average values stated because of room reflections and other nearby noise sources. The declared sound-power levels indicate an upper limit, below which a large number of computers will operate.
Electrical input requirements	● Sine-wave input (47–63 Hz) required ● Input voltage low range: – Minimum: 100 V AC – Maximum: 127 V AC ● Input voltage high range: – Minimum: 200 V AC – Maximum: 240 V AC ● Input kilovolt-amperes (kVA), approximately: – Minimum: 0.194 kVA – Maximum: 0.700 kVA
Front connectors	Two USB Video
Back connectors	● Two Ethernet (RJ 45). Optionally, two or four additional Ethernet. ● Serial ● Two USB ● Video ● Systems management Ethernet (IMM)

Server components

Component	Minimum Specification	Upgrade options based on product requirements
Microprocessor	One Intel E5520 quad core, 2.26 GHZ processor	No additional options
Memory	12 GB of 1333 Mhz, fullybuffered DDR-3 RDIMMs (Two 2GB DIMMs):	No additional options
Media drive	DVD-R/W SATA slimline	No additional options
Hard disk drive expansion bays	Six 2.5-inch hot-swap SAS hard disk drive bays	No additional options
Hard disk drive	Two 146 GB SAS 2.5" 10K RPM hard drives	No additional options
RAID controllers	ServeRAID-MR10i RAID SAS adapter that provides RAID level 5. Includes 256 MB cache module and battery for write cache	No additional options
PCI expansion slots	Two PCI Express x16 Gen 2 slots: ● Slot 1 supports a low profile DUAL NIC card (half height, half-length cards) ● Slot 2 supports full height, half-length cards	No additional options
Hot-swap fans	Six	No additional options

Component	Minimum Specification	Upgrade options based on product requirements
Power supply	One 675W, 12V AC power supply	Redundant 675W, 12V AC power supply
Video controller	Integrated Matrox G200 (two analog ports, one front and one back, that can be connected at the same time) The maximum video resolution is 1280 x 1024 at 75 Hz. ● SVGA compatible video controller ● DDR2 250 MHz SDRAM video memory controller ● Avocent Digital Video Compression ● Video memory is not expandable	No additional options

Environmental requirements

Server status	Air temperature	Maximum Altitude	Relative humidity
Server on	● 10 to 35º C (50 to 95º F) at altitude of up to 914.4 m (3,000 feet) ● 10 to 32º C (50 to 90º F) at altitude of 914.4 m to 2,133 m (3,000 to 7,000 feet)	2,133 m (7,000 feet)	8% to 80%
Server off	10°C to 43°C (50.0°F to 109.4°F)	2,133 m (7,000 feet)	8% to 80%

Appendix D: Network services on Communication Manager servers

Network service and port information for S8400 server, S8500 series server and S8700 series server can be obtained via the Avaya Support site http://support.avaya.com.

Appendix E: Additional security resources

Documents mentioned in this security guide

This Communication Manager security guide mentions the documents that are listed in Table 54: Communication Manager documents on page 249.

Table 54: Communication Manager documents

Document title	Document Number
Administration for the Avaya G250 and the G350 Media Gateways (03-300436)	03-300436
Administering Avaya Aura™ Communication Manager (03-300509)	03-300509
Administering Network Connectivity on Avaya Aura™ Communication Manager (555-233-504)	555-233-504
Avaya Application Solutions: IP Telephony Deployment Guide (555-245-600)	555-245-600
Avaya Toll Fraud and Security Handbook (555-025-600)	555-025-600
Avaya Aura™ Communication Manager Feature Description and Implementation (555-245-205)	555-245-205
Avaya Aura™ Communication Manager Hardware Description and Reference (555-245-207)	555-245-207
Installing and Upgrading the Avaya S8300 Server (555-234-100).	555-234-100
Installing and Upgrading the Avaya G700 Media Gateway (03-603333)	03-603333
Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers (03-300431)	03-300431
Maintenance Procedures for Avaya Aura™ Communication Manager, Media Gateways and Servers (03-300432)	03-300432
Maintenance Alarms for Avaya Aura™ Communication Manager, Media Gateways and Servers (03-300430)	03-300430
	1 of 2

Table 54: Communication Manager documents

Document title	Document Number
SNMP Reference Guide for Avaya Communication Manager (03-602013)	03-602013
4600 Series IP Telephone LAN Administrator Guide (555-233-507)	555-233-507
	2 of 2

Security documents on the Avaya Support site

Security-related documents that complement this security guide are listed in Table 55: Security related Communication Manager documents on page 250.

Table 55: Security related Communication Manager documents

Document title	Link
Access Security Gateway family of security products	http://support.avaya.com/japple/css/japple?PAGE=Product&temp.productID=107697.
Application Note: G350 and G250 R3.0 IPSec VPN	http://support.avaya.com/elmodocs2/g350/AppNotes_G350_G250_R3_ndezent_070605.pdf
Avaya Enterprise Services Platform Security Overview	Requires non-disclosure agreement
Avaya Interactive Response Security	http://support.avaya.com/elmodocs2/ir/r2_0/print_Security.pdf
Avaya's Security Vulnerability Classification	http://support.avaya.com/elmodocs2/security/security_vulnerability_classification.pdf
Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework	http://www.bis.org/publ/bcbs128.pdf
Communication Manager Administrator Logins White Paper	http://support.avaya.com/elmodocs2/white_papers/CM_Administrator_Logins.pdf
	1 of 2

Table 55: Security related Communication Manager documents

Document title	Link
Downloading Avaya 46xx IP Telephone Software Using Avaya Media Servers	http://support.avaya.com/elmodocs2/white_papers/TFTP_HTTP_Download_External_060504.pdf
Firmware Download Procedures	ftp://ftp.avaya.com/incoming/Up1cku9/tsoweb/firmware/TNpackFirmwareDownloadInstructions.pdf
J-series Services Router Administration Guide	http://www.juniper.net/techpubs/software/jseries/junos82/jseries82-admin-guide/jseries82-admin-guide.pdf
RedSky E911 Overview	http://www.redskytech.com/documents/E911_Manager_Overview.pdf
Verasmart Technologies CDR products	http://www.veramark.com/products/verasmart.htm
	2 of 2

Index