



Avaya Aura® Communication Manager Security Design

Release 5.2

03-601973
Issue 3
August 2009

© 2009 Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full legal page information, please see the complete document, Avaya Legal Page for Hardware Documentation, Document number 03-600759.

To locate this document on our website, simply go to <http://www.avaya.com/support> and search for the document number in the search box.

Documentation disclaimer

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

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

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

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

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

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

Introduction	9
Information classifications and NDA requirements	9
Disclaimer	9
How this book is organized	10
Communication Manager security philosophy overview	11
Who is responsible for Communication Manager security?	11
How this guide complements other Avaya product security guides	12
Chapter 1: Secure by Default	13
Secure by design	13
Secure by default	14
Secure communications	15
Why Avaya chose the Linux operating system for Communication Manager. . .	17
How Avaya modifies Linux to improve security	17
More information.	19
Why using SSH/SCP is more secure than Telnet, FTP, or SNMP	19
Disabled by default	19
Avaya Services.	20
Planning against viruses and worms and other malicious code	20
DoS methods Avaya has designed against	21
Additional information.	23
Security problems addressed by digital certificates	24
Additional information.	24
How signed firmware provides data integrity assurance	24
Additional Information.	25
Access profiles	25
System Management Interface default profiles and permissions	26
Communication Manager default SAT profiles and permissions	31
Privilege escalation	33
Additional information.	33
Local host account authentication	34
What is host intrusion detection?	35
Tripwire.	35
Tripwire database	35
Tripwire report	37
Additional information.	37

Chapter 2: Configurable Security	39
Avaya's encryption overview	39
Transport and storage encryption algorithms	40
IPSI link security	41
H.248 link security	42
H.225.0 Registration, Admission, and Status (RAS)	42
H.225.0 call signaling	43
RTP media encryption	43
Media gateway support	45
Desk phones and client endpoint support	46
How does media encryption interact with other features?	48
Encryption summary	50
Additional Information	54
Administering encryption in Avaya solutions	55
SAT administration for IP CODEC Sets and Network Regions	55
SAT administration for signaling groups	59
Network Region Wizard	60
Additional information	60
Mixing encrypted and non-encrypted policies	60
Additional information	61
Chain of trust	61
Avaya Public Key Infrastructure	62
Avaya certificate components	63
PKI in Communication Manager	64
Customers can install their own trusted certificates	65
PKI in H.323 and SIP endpoints	66
Connection to Communication Manager Web interface	68
Filesync to duplicated or survivable servers	69
Managing changes to the Avaya certificate	69
Additional information	70
Credentials complexity and expiration requirements	71
Password complexity policies	71
Credentials expiration and lockout policies	72
Password administration recommendations	74
Credentials management	74
More information	74
Applying profiles for role-based administration	75
Creating the privileged administrator account	76
More information	78

Managing administrative accounts	79
Account administration recommendations	79
Administering authentication passwords	80
Access Security Gateway (ASG)	80
ASG Guard and ASG Guard Plus	81
ASG Guard II	81
ASG Guard and ASG Guard II compared.	82
ASG security products	83
Limiting long-distance access	83
Configuring SNMP and syslog	84
What security-related events are logged?	84
Configuring SNMP in Communication Manager.	85
Configuring the syslog server in Communication Manager	90
Accessing system logs through the Web	95
More information.	96
Chapter 3: Network Security Integration.	97
Administering firewall settings in Communication Manager	97
Default Communication Manager firewall settings	97
Separation of network functionality	100
Control and bearer signaling separation.	100
Control and bearer signaling in VLANs	101
Layer 2 and Layer 3 hardening	101
GRE tunneling	102
IPSec VPN	102
Access control lists	104
Access control list rule specifications	104
External authentication of server administrator accounts	105
External authentication accounts	106
External authentication servers	107
Administering external authentication	109
Additional information.	110
802.1X and LLDP.	110
Designing VLAN groups for functional network segmentation.	110
Traffic filtering and firewalling	111
Assigning VLANs in Communication Manager	112
Assigning VLANs in the G250-series, G350, G430 and G450 Media Gateways	112
How ARP spoofing facilitates network attacks	112
Security strategies to combat ARP spoofing	113

Contents

Security vulnerabilities with name and address management	113
DHCP vulnerabilities.	114
DHCP security	114
DNS vulnerabilities	115
DNS security	116
How Communication Manager addresses NIST recommendations	116
Confidentiality and privacy	116
Integrity issues.	119
Availability and Denial of Service.	120
Recommendations for preventing DoS attacks	121
Mitigating call processing overloads.	121
Remote Managed Services	122
Signaling groups.	124
More information.	125
Chapter 4: Operational Security	127
What is an Avaya Security Advisory	127
How do I get Avaya Security Advisories?	128
How to interpret an Avaya Security Advisory	129
How an advisory is organized	130
How Avaya incorporates security updates in its applications	131
Removing old accounts	132
Restricting Web access to system logs	132
Where is security information logged?	132
Interpreting the syslog header	133
Interpreting SNMP entries in the syslog	134
Interpreting the platform command history log	135
Interpreting Communication Manager security violations	136
Interpreting the command history log for Communication Manager SAT	139
Interpreting the command history log for Web activity	141
How Avaya delivers security updates	146
Validating a security update	147
Applying an operating system security update	147
Applying an Avaya field load or software update	148
Determining the contents of a security update	148
Considerations for customers who must comply with the Sarbanes-Oxley Act	150
Communication Manager data used for financial purposes	151
Other adjunct systems collecting Communication Manager data	152

Considerations for customers who must comply with the Graham-Leach-Bliley Act.	152
Considerations for customers who must comply with HIPAA	153
Considerations for customers who must comply with CALEA.	155
Considerations for customers who must comply with FISMA	156
Considerations for customers who want to comply with ISO 17799.	157
Considerations for customers who must comply with E911	160
Communication Manager compliance with 911	161
Considerations for non-US customers who must comply with regulations. . . .	162
Basel II	162
Common Criteria.	162
Secure backups of Communication Manager data and translations.	164
Secure updates of Avaya software and firmware	164
Remote monitoring and maintenance	165
SSDP firewall and wireless access.	166
Remote password complexity and expiration parameters	166
Appendix A: Physical Interfaces and Associated Network Services . .	167
Avaya S8300 Server	167
TN8300C access / connectivity	168
Avaya S8400 Server	168
TN8400AP access / connectivity	169
Avaya S8500 Series Servers	175
S8500 access / connectivity.	175
S8510 access / connectivity.	178
Server Availability Management Processor	179
Modem	179
S8510 connections	180
Avaya S8700 Series Servers	181
Memory and software duplication	182
Fiber link between the active and standby servers	183
S8720 access / connectivity.	192
S8730 access / connectivity.	194
Appendix B: Network Services on Communication Manager Servers. .	197
Appendix C: Additional Security Resources	198
Documents mentioned in this security guide	198
Security documents on the Avaya support site	199

Index **201**

Introduction

Information classifications and NDA requirements

This book is designed to provide a certain level of security-related information that Avaya divides into these four information classifications:

Classification	Description
Avaya Restricted	This classification is for extremely sensitive business information, intended strictly for use within Avaya. Its unauthorized disclosure could have a severe adverse impact to Avaya or its customers, Business Partners, and/or suppliers.
Avaya Confidential	This classification applies to less sensitive business information intended for use within Avaya. Its unauthorized disclosure could have significant adverse impact to Avaya or its customers, Business Partners, and/or 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 classifications above and is considered sensitive only outside the Avaya. While disclosure might not have a serious adverse impact on Avaya or its customers, Business Partners, and/or suppliers, it is Avaya's information and unauthorized disclosure is against policy.
Public	This classification applies to information explicitly approved by Avaya management as non-sensitive 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 website. 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 used 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, express or implied.

How this book is organized

In addition to this introduction *Avaya Aura® Communication Manager Security Design* contains four major sections and three appendices that are described in [Table 1](#)

Table 1: Communication Manager security guide

Chapter / section	Description
Introduction	<ul style="list-style-type: none"> • Communication Manager security philosophy overview on page 11 • How this guide complements other Avaya product security guides on page 12
Secure by Default	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.
Network Security Integration	Discusses how to integrate Avaya products securely into an exiting network by leveraging resources such as LDAP, Active Directory, Firewalls, etc.
Operational Security	Discusses ongoing activities useful to ensure a high level after the solution has been deployed. Areas include patching, logging, monitoring, etc.
Appendices	<ul style="list-style-type: none"> • Appendix A: Physical Interfaces and Associated Network Services <ul style="list-style-type: none"> - Avaya S8300 Server on page 167 - Avaya S8400 Server on page 168 - Avaya S8500 Series Servers on page 175 - Avaya S8700 Series Servers on page 181 • Appendix B: Network Services on Communication Manager Servers • Appendix C: Additional Security Resources <ul style="list-style-type: none"> - Documents mentioned in this security guide on page 198 - Security documents on the Avaya support site on page 199

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 violations 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 127 and [How do I get Avaya Security Advisories?](#) on page 128.

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, and data backups and/or 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

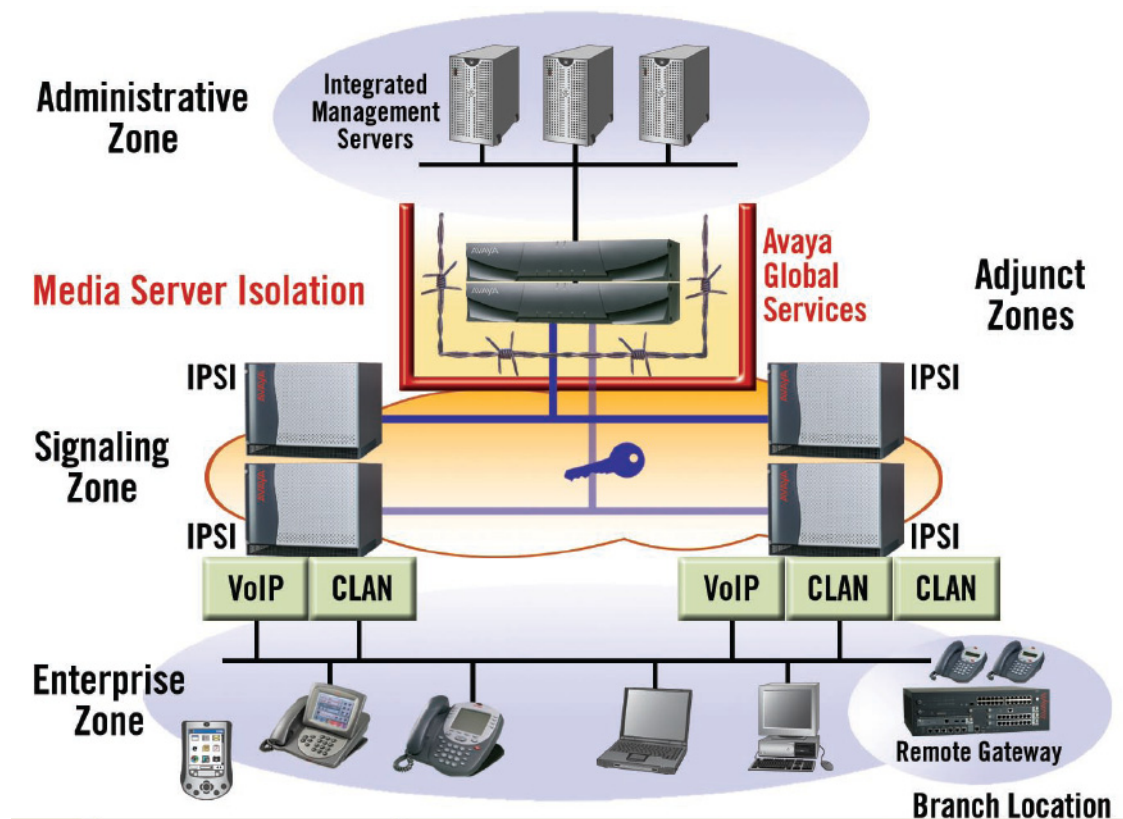
Chapter 1: Secure by Default

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, denial of service (DOS) and malicious attacks.

As can be seen in the diagram below, 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



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 purely accommodate the data they are built for. This provides protection against attacks from within the enterprise and branch office zone. The diagram above 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.

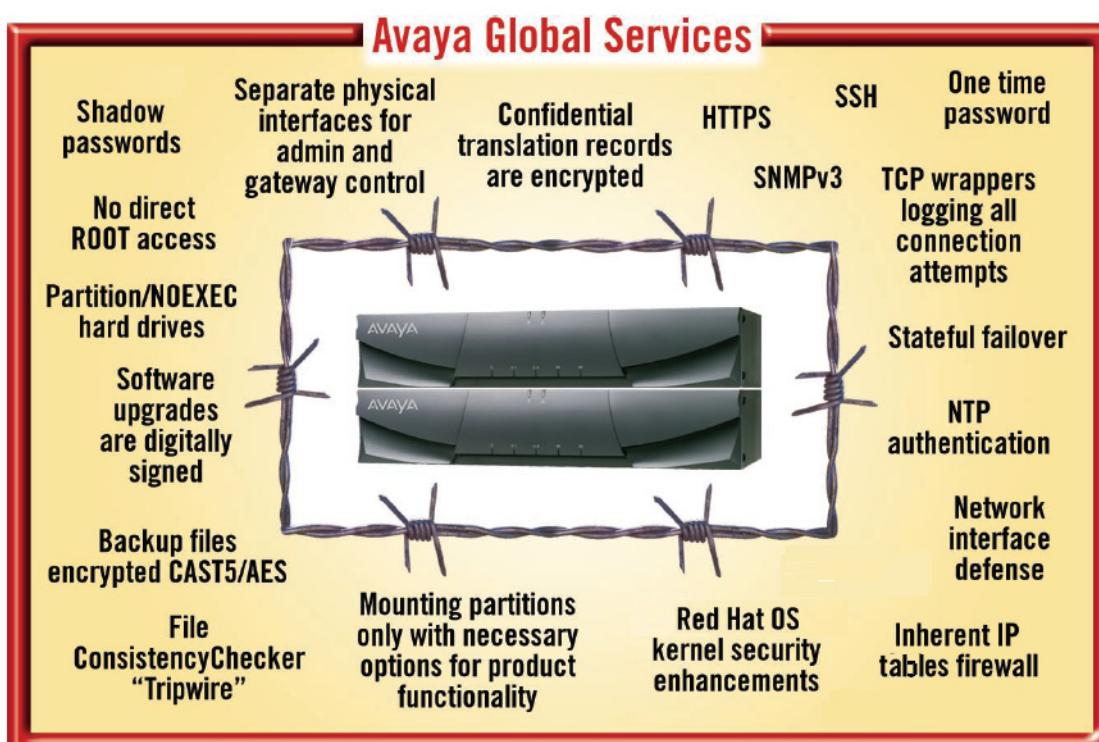
Gateways with dedicated gatekeeper front end interfaces (CLAN) inspect the traffic and protect the Media Server zone from flooding attacks, malformed IP packets, and attempts to gain unauthorized administrative access of the Media Server via the Gateways.

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.

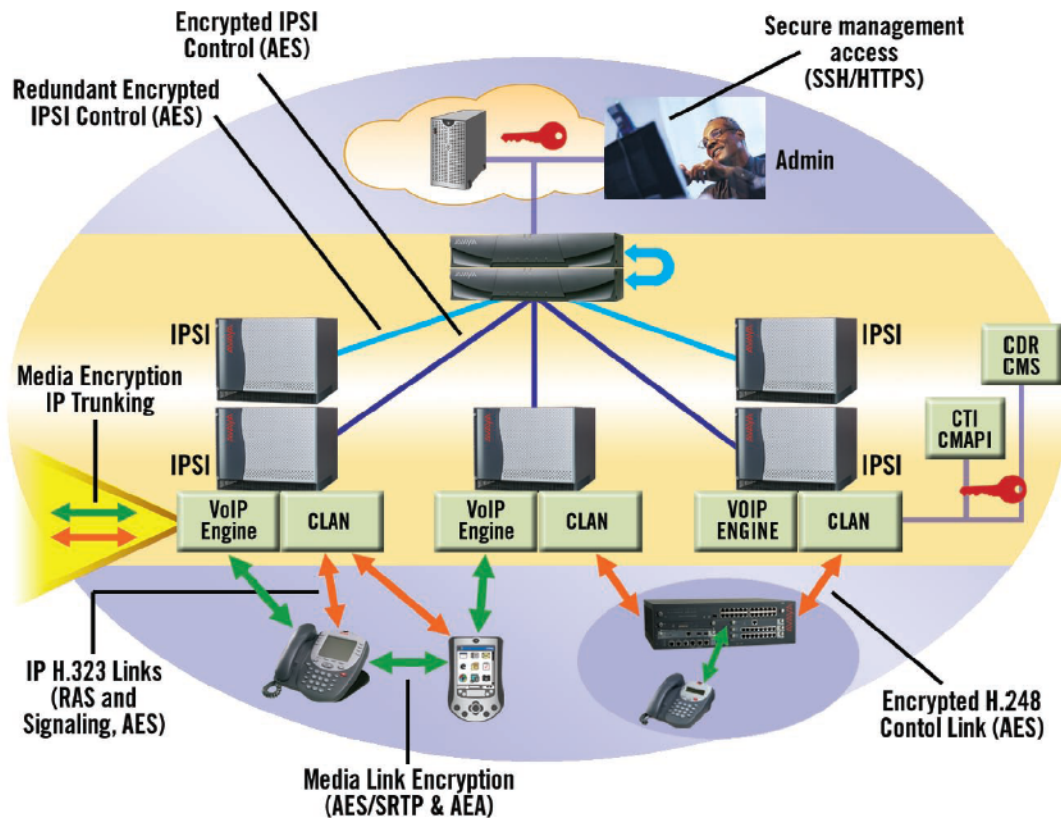


Communication Manager provides a range of in-built functionality to address the threats posed by malicious software. This functionality minimizes the need for co-resident anti-virus software, which can interfere with efficient call processing and require continuous administrative attention to ensure anti-virus 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.



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](#) on page 17
- [Why using SSH/SCP is more secure than Telnet, FTP, or SNMP](#) on page 19
- [Planning against viruses and worms and other malicious code](#) on page 20

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.

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. 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 19), 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 20) 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.

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.

More information

- [DoS methods Avaya has designed against](#) on page 21

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 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 TLS or 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. [Table 2](#) lists the security impacts of viruses and worms.

Table 2: Security impacts of viruses and worms

Security implementation	Security impact
Natural immunity	Avaya's Linux-based servers <i>do not</i> support: <ul style="list-style-type: none"> • 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 3rd-party, host-based antivirus products on its Linux-based servers and uncovered significant performance degradation attributable to the 3rd-party software. Avaya does not recommend installation of such products on its Linux-based servers.
Antivirus products	Customers have successfully used 3rd-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](#) on page 21

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 3](#) without loss of sanity, without rebooting or restarting, and without reloading, and automatically recover to full service after the DoS attack.

Table 3: 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 host 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	<p>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</p> <ul style="list-style-type: none"> • 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 3: 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 121

Digital certificates

- [Security problems addressed by digital certificates](#) on page 24
- [How signed firmware provides data integrity assurance](#) on page 24

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 24
- [Avaya Public Key Infrastructure](#) on page 63
- [Secure updates of Avaya software and firmware](#) on page 164

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 63
- [Secure updates of Avaya software and firmware](#) on page 164

Secure administration

- [Access profiles](#) on page 25
- [External authentication of server administrator accounts](#) on page 105

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 4: Communication Manager System Management Interface default profiles](#) on page 26 lists and describes the intended use of the default profiles for the System Management Interface.

Table 4: Communication Manager System Management Interface default profiles

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

Table 4: Communication Manager System Management Interface default profiles

Profile number	Group ¹	Description
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		

1. Members of the **susers** Linux group have full access to all Web pages; **users** have access to a limited subset of these pages.

System Management Interface default settings

Access permissions to the System Management Interface are administered on the **Security > Web Access Mask** page. [Table 5: Communication Manager Web Access Mask default settings](#) on page 27 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 5: Communication Manager Web Access Mask default settings

Menu-Item	Fixed (suser)	Editable (user)
	Profile 18	Profile 19
Initial Menu		
Avaya Installation Wizard	X	X
Network Region Wizard	X	X
1 of 4		

Table 5: Communication Manager Web Access Mask default settings

Menu-Item	Fixed (suser)	Editable (user)
	Profile 18	Profile 19
Native Configuration Manager	X	X
Maintenance Web Interface	X	X
Upgrade Tool	X	
Alarms		
Current Alarms	X	X
SNMP Agents	X	
SNMP Traps	X	
Filters	X	
Diagnostics		
Restarts	X	X
System Logs	X	X
Temperature/Voltage	X	
Ping	X	
Traceroute	X	
Netstat	X	
Modem Test	X	
Network Time Sync	X	
Server		
Status Summary	X	X
Process Status	X	
Shutdown Server	X	
Server Date/Time	X	
Software Version	X	X
Server Configuration		
2 of 4		

Table 5: Communication Manager Web Access Mask default settings

Menu-Item	Fixed (suser)	Editable (user)
	Profile 18	Profile 19
Configure Server	X	
Restore Defaults	X	
Eject CD-ROM	X	
Server Upgrades		
Manage Software	X	
Make Upgrade Permanent	X	
Boot Partition	X	
Manage Updates	X	
IPSI Firmware Upgrades		
IPSI Version	X	X
Download IPSI Firmware	X	
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 PC Card	X	
Security		
Administrator Accounts	X	
3 of 4		

Table 5: Communication Manager Web Access Mask default settings

Menu-Item	Fixed (suser)	Editable (user)
	Profile 18	Profile 19
Change Password	X	X
Login Reports	X	
Modem	X	
Server Access	X	
Syslog Server	X	
License File	X	
Authentication File	X	
Firewall	X	
Tripwire	X	
Tripwire Commands	X	X
Install Root Certificate	X	X
SSH Keys	X	
Web Access Mask	X	
Media Gateways		
Configuration	X	
Miscellaneous		
File Synchronization	X	
IP Phones	X	
Download Files	X	
CM Phone Message File	X	
Serial Numbers	X	
4 of 4		

Communication Manager default SAT profiles and permissions

Communication Manager default SAT profiles

[Table 6: Communication Manager default profiles](#) on page 31 lists and describes the default profiles for the SAT interface.

Note:

Co-resident applications such as CM Messaging or Octel voice mail adjuncts require a standard profile to support TSC access to Communication Manager.

Table 6: Communication Manager default profiles

Profile number	Profile name	Permissions/access	Notes
0	Services superuser	Equivalent to the former SAT <i>init</i> 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 <i>inads</i> login	Cannot be edited, copied, viewed, or removed. Requires a second user authentication by Communication Manager.
2	Business Partner	Equivalent to the former SAT <i>dadmin</i> 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 <i>craft</i> login	Cannot be edited, copied, viewed, or removed. Requires a second user authentication by Communication Manager.
1 of 2			

Table 6: Communication Manager default profiles (continued)

Profile number	Profile name	Permissions/access	Notes
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.
18	Customer superuser	Equivalent to the former SAT default <i>customer super-user</i> login	Cannot be edited or removed.
19	Customer user	Equivalent to the former SAT default <i>non-super-user customer</i> 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).

add user-profile n
Page 1 of X

User Profile N

User Profile Name: Example Profile

This profile is disabled? n

Facility Test Call Notification? n

Grant un-owned permissions? n

Shell Access?n

Acknowledgement required?n

Extended Profile?n

Name	Cat	Enbl
Adjuncts	A	n
Call Center	B	n
Features	C	n
Hardware	D	n
Hospitality	E	n
IP	F	n
Maintenance	G	n
Measurements and Performance	H	n
Remote Access	I	n

Name	Cat	Enbl
Routing and Dial Plan	J	n
Security	K	n
Servers	L	n
Stations	M	n
System Parameters	N	n
Translations	O	n
Trunking	P	n
Usage	Q	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

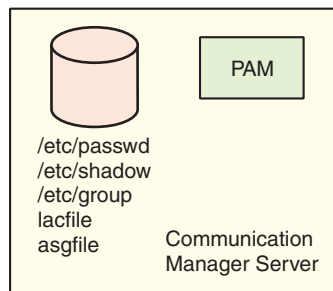
- [Credentials complexity and expiration requirements](#) on page 72

- [Managing administrative accounts](#) on page 80
- [Administering authentication passwords](#) on page 81

Local host account authentication

Communication Manager is configured by default to support only local host accounts as shown in [Figure 1: 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 1: 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.

Intrusion detection

- [What is host intrusion detection?](#) on page 35
- [Tripwire](#) on page 35

What is host intrusion detection?

An intrusion detection system (IDS) monitors operating systems and applications for some of the most widely-used hacking techniques:

- Unauthorized changes to system files
- Altering configuration files
- Replacing or infecting binaries
- Downloading new executables
- Creating unauthorized files and directories

Communication Manager uses the Tripwire IDS to monitor these types of files:

- Executable files (with the .exe suffix)
- .conf ("dot-conf") or configuration files
- /etc/passwd, /etc/shadow, /etc/opt/ecs/agsfile, and /ect/opt/ecs/lacfile (application-specific files)

Tripwire

Tripwire is a host-based intrusion detection system (IDS) that monitors the filesystem for changes. Based on the presumption that an intruder who gains root access would probably make changes to the system somewhere, Tripwire

- Monitors various filesystem parameters
- Compares the parameters against a stored database
- Alerts the user of any changes

For the greatest level of assurance run Tripwire in a "clean" environment, that is, immediately after installing Linux and applying security updates but before connecting equipment to the network.

Tripwire database

Tripwire monitors file integrity by maintaining a database of cryptographic signatures for programs and configuration files installed on the system. This database contains checksums and other characteristics for the files using the rules specified in the configuration file, also called a policy file, that defines the characteristics for each tracked file.

The database file (/var/lib/tripwire/s8xxx.twd) is owned by root and can be modified only by root. The database filename depends on the Communication Manager server model, for example, the filename for an Avaya S8720 Server is "s8720.twd." Using this filename as an example, more information about the database can be obtained by issuing the `twadmin -m e s8720.twd` at the server command line interface (CLI) with the following output:

```
File: "/var/lib/tripwire/s8720.twd"
File Type: Tripwire Database (Ver 2.2.0.0)
Encoding: Asymmetric Encryption
The following keys decrypt this file:
  Local Keyfile: /etc/tripwire/s8720-local.key
```

The cryptographic signatures that Tripwire uses to prevent writing files require the private key, which is encrypted with a secret passphrase. The public key that is required to read files is available to all users and is located in /etc/tripwire/s8xxx-local.key.

The Tripwire policy file (/etc/tripwire) is owned by root and can be modified only by root. Examples of files and directories that Tripwire monitors include:

- System binaries (/bin, /sbin, /lib, and /usr/bin)
- Linux system files (/home, /usr, /selinux, and /srv)
- Boot files (/boot)
- Linux configuration files (/etc)
- Root files (/root)
- Var files (/var)
- Critical devices (/proc, /sys)
- Communication Manager configuration files (asgfile, lacfile, /backup)
- Communication Manager executable files (/opt, /release)
- Special files in which the INODE (Index **NODE** or Identification **NODE**) number might change:
 - /etc/ntp/drift
 - /etc/issue.net
 - etc/ld.so.cache
 - /etc/mstab

Note:

Although Tripwire monitors changes to files that are *expected* to change, Communication Manager purposely excludes files that routinely change from Tripwire monitoring.

To view the policy file run the `twadmin -m p` command at the server CLI. The output file shows "rulenames" (for example, Linux System, Critical System Boot Files, Linux Config Files, and many others) and the monitored directories for each rulename.

Tripwire report

Tripwire monitoring compares file attributes with those in the reference database, and the Tripwire report lists the discrepancies and modifications to monitored files. The Tripwire report is restricted to **craft** permissions and above and is available from the System Management Interface by selecting **Security > Tripwire Commands**.

Additional information

- *Maintenance Procedures for Avaya Aura® Communication Manager, Media Gateways and Servers (03-300432)* for information on how to generate and interpret a Tripwire report.
- Red Hat Tripwire documentation at: <http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/ch-tripwire.html>

Chapter 2: Configurable Security

Encryption

- [Avaya's encryption overview](#) on page 39
- [Transport and storage encryption algorithms](#) on page 40
- [Administering encryption in Avaya solutions](#) on page 56
- [Mixing encrypted and non-encrypted policies](#) on page 61

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 7](#) compares how encryption mitigates the vulnerabilities in signaling and bearer media.

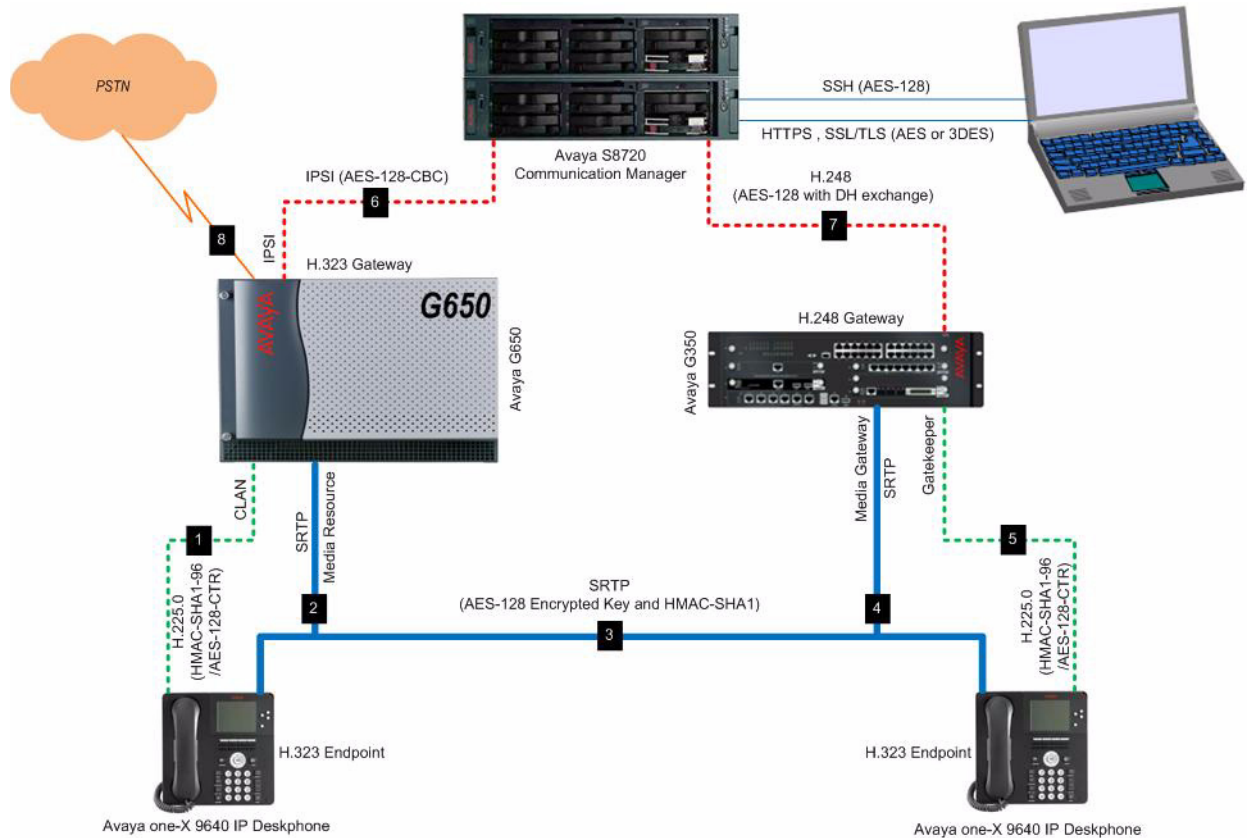
Table 7: Comparisons in signaling and bearer traffic

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 2: Encrypted links in Communication Manager enterprise](#) on page 41 shows the encrypted links in a Communication Manager enterprise.

Figure 2: 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 41 (Note 6)
- [H.248 link security](#) on page 42 (Note 7)
- [H.225.0 Registration, Admission, and Status \(RAS\)](#) on page 42 and [H.225.0 call signaling](#) on page 43 (Notes 1 and 5)
- [RTP media encryption](#) on page 43 (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 of [Figure 2](#).

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

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 8: 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.
1 of 2		

Table 8: Encryption supported in Communication Manager

Encryption Technique	Available algorithms	Description
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
	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 9: Encrypted supported in Avaya media gateways

Model	Version	Supported encryption algorithms
TN2302AP (Medpro)	N/A	Supports AEA or AES <ul style="list-style-type: none"> Extra DSP utilization using AES variant. AES reduces circuit-switched-to-IP call capacity by 25%.¹
TN2602AP (IP Media Resource 320)	SRTP support	Supports AEA, or AES, and SRTP <ul style="list-style-type: none"> Does not utilize "extra DSPs" for either method chosen.
1 of 21 of 2		

Table 9: Encrypted supported in Avaya media gateways

Model	Version	Supported encryption algorithms
TN2312BP (IPSI)		AES-128-Cipher Block Chaining
H.248 Media Gateways (G350, G450, G430, G250)		Supports AEA, or AES (128-Output FeedBack), and SRTP <ul style="list-style-type: none"> • Extra DSP Utilization using Avaya Media Encryption AES variant (differs based in Media Gateway) • Extra DSP utilization using SRTP
2 of 22 of 2		

1. Administering Network Connectivity on Avaya Aura® Communication Manager http://support.avaya.com/elmodocs2/comm_mgr/r4_0/pdfs/233504_12.pdf, p. 251.

Desk phones and client endpoint support

Table 10: 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 11 .	Supports AEA or AES
Avaya 46xx (SIP firmware)	N/A	Does not support any form of Media Encryption
1 of 2		

Table 10: Encryption supported in Avaya endpoints

Model	Version	Detail
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
2 of 2		

Table 11: 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 12](#):

Table 12: 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: <ul style="list-style-type: none"> • 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 13: 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).
SNMPv3 agent	DES-CBC (56-bit), HMAC-SHA-1-96, HMAC-MD5-96
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.
CNA test plug	Gateway use AES-ECB (128-bit) to protect all communication between CNA test plug and remote CNA scheduler. It uses UDP. Initial symmetric key negotiation is done over TLS tunnel where the CNA test plug acts as TLS client.
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 14](#) 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 14: 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 14: 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. ¹ Keys are not escrowed but are stored in RAM where they are not accessible by administrators or users.
				2 of 4

Table 14: 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 ² but not accessible by users or administrators exchanged with 128-bit Diffie-Hellman.
				3 of 4

Table 14: 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. ³	SCP	AES-128	15-256 character pass phrase
				4 of 4

1. 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. 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. For manual movement to another server running the same Communication Manager release.

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, pp. 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

Page1 of 2

IP Codec Set

Codec Set: 1

	Audio Codec	Silence Suppression	Frames Per Pkt	Packet 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 15: Communication Manager administrable encryption algorithms](#) on page 58.



Important:

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.

Note:

SRTP encryption is supported by 96xx telephones only.

Table 15: 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: <ul style="list-style-type: none"> • Server-to-gateway (H.248) • Gateway-to-endpoint (H.323)
aea	Avaya Encryption Algorithm. Use this option as an alternative to AES encryption when: <ul style="list-style-type: none"> • 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-hmac80¹	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
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)

1. The only supported SRTP value for stations is **srtp-aescm128-hmac80**. H.323 IP trunks support all eight of the listed SRTP algorithms.

The second part of administering Communication Manager encryption involves assigning codec(s) 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
                                Use Default Server Parameters? n
DIFFSERV/TOS PARAMETERS              Server IP Address: . . .
    Call Control PHB Value: 34          Server Port: 5055
    Audio PHB Value: 46
    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 non-encrypted policies](#) on page 61 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:
Calls Share IP Signaling Connection? n

LRQ Required? n                        Bypass If IP Threshold Exceeded? n
RRQ Required? n                      H.235 Annex H Required? n
Media Encryption? y                  Direct IP-IP Audio Connections? y
Passphrase:                          IP Audio Hairpinning? n
DTMF over IP: out of band            Interworking Message: PROGRESS
Link Loss Delay Timer(sec): 90        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 through 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 non-encrypted policies](#) on page 61
- “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 non-encrypted policies

[Administering encryption in Avaya solutions](#) on page 56 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 non-encrypted 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 56
- “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)*

Digital certificates and server trust relationships

- [Chain of trust](#) on page 62
- [Avaya Public Key Infrastructure](#) on page 63
- [PKI in Communication Manager](#) on page 65
- [Managing changes to the Avaya certificate](#) on page 70

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 RFA license 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 standard license file.

Avaya RFA uses a

- Crypto-accelerator board to store the private key of the IA and to sign the 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. To goal is to conduct electronic business, confident 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.

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

[Table 16](#) lists the Avaya public and private keys and their uses.

Table 16: Key pair and certificate usage

Entity	Key type	Uses
Subscriber	Private key	<ul style="list-style-type: none"> ● Digital certificates ● Encryption <p>In some cases the subscriber private key is used specifically for signing code.</p>
Relying party	Public key	<ul style="list-style-type: none"> ● 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 certificate components

The Avaya Product Certificate Authority issues signed identity certificates for customer-purchased Avaya products, automatically-generated through the RFA license process that:

- Authenticates the end-customer
- Distributes the customer-specific certificate and private key.

Note:

To replace an identify certificate, you must generate a new Communication Manager license at the RFA site and install it on the Communication Manager server.

[Table 17](#) lists the fixed components that are common to all certificates issued by the Avaya Product Certificate Authority. These components are used to identify the namespace that the CA can sign.

Table 17: Avaya product certificate components

Component	Value	Description
Name	Avaya Inc.	Indicates that Avaya issues the certificate
Organizational Unit (OU) ¹	Avaya Enterprise Wide Licensing	For certificates issued by Avaya Enterprise Wide Licensing
	Communication Manager	For certificates issued for Communication Manager
	<Product Name>	For certificates issued to a product; provides easy and public identification with the OU name <Product Name>
Common name (CN)	Communication Manager: <ul style="list-style-type: none"> • ESID • SID • MID 	Identifies the certificate subject, for example, the Avaya Business Unit, Product House, or Product along with additional information that makes the common name unique.

1. The first OU listed must be described in this table.

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 3rd-party certificate ([Customers can install their own trusted certificates](#) on page 66).
- Establish connections between IP phones and Communication Manager through Avaya's trusted chain ([PKI in H.323 and SIP endpoints](#) on page 67) 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 70).
- Authenticate access to the Communication Manager Web interface ([Connection to Communication Manager Web interface](#) on page 69)
- SIP/TLS connections
 - Management
 - Signaling

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 71) at the server command line, customers can load a 3rd-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 3rd-party certificate.

The **all-ca.crt** file can contain up to eight (8) certificates, meaning that the customer may load up to 4 additional 3rd-party certificates. If more than 8 certificates are in the **all-ca.crt** file, Communication Manager loads the first 8 then ignores the remaining certificates and generates a minor alarm (see [Additional information](#) on page 71) and a syslog entry to notify the user that it could not load the file.

3rd-party certificate management

[Table 18](#) describes how Communication Manager handles 3rd-party certificates.

Table 18: Communication Manager 3rd-party certificate management

Activity	Description
File sync	To prevent overwriting a customer-installed, 3rd-party certificate, file sync does not synchronize any certificates.
Upgrades	<ol style="list-style-type: none"> 1. Copy the 3rd-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 3rd-party certificate with the tlscertmanage command. <p>Note:</p> <p>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.</p>
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](#) 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 ¹	Download configuration files ² port trusted certificates
46XX (H.323)	Avaya Product Root Certificate Authority Trust Certificates ¹	Download configuration files ² Import trusted certificates
16XX (H.323)	Avaya Product Root Certificate Authority	Download configuration files ²
1 of 2		

Table 19: Certificate usage in Avaya endpoints

Phone type	Certificate	Use/Description
96XX SIP	Avaya Product Root Certificate Authority ³ x.509 Identity Certificate ⁴	Download configuration files over HTTPS, when enabled ⁵ Establishes a SIP/TLS connection to the Avaya SIP Enablement Services (SES) server ⁶ and utilized if 802.1X EAP/TLS is enabled.
SIP Softphone	Hard-coded certificate	SIP Softphone firmware includes a default phone certificate ⁷ .
2 of 2		

1. Beginning with 46XX H.323 Release 2.9 firmware and 96XX H.323 Release 2.0 firmware customers can import trusted 3rd-party certificates to the phone using the TRUSTCERT parameter.
2. Includes 46xxsettings.txt, 46xxupgrade.scr, 96xxupgrade.txt, etc. downloaded through the Communication Manager HTTPS server.
3. 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.
4. Customers can replace the default identify certificate using the Simple Certificate Enrollment Protocol (SCEP, see [Additional information](#) on page 71).
5. Uses TLSSRV, TSLPORT, HTTPSRRV, and HTTPPORT parameters in the DHCP Option #242.
6. The TLS connection from the SIP phone to the SIP Enablement Services (SES) server is encrypted using TLS_RSA_WITH_AES_128_CBC_SHA.
7. However, Avaya recommends using a uniquely-provisioned phone certificate installed through Simple Certificate Enrollment Protocol (SCEP, see [Additional information](#) on page 71).

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 customer has 30 days to obtain a customized Communication Manager license file from the Remote Feature Activation (RFA) website. Avaya's secure installation and provisioning process assures that the RFA license file distributions, including the certificates, are valid. 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 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](#) 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.
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	<p>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.</p> <p>A certificate is revoked in these circumstances:</p> <ul style="list-style-type: none"> • 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.
1 of 2	

Table 20: Changes in the Avaya certificate

Type of change	Description
Who can request revocation?	<p>Certificate revocations can be requested by:</p> <ul style="list-style-type: none"> • 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 <p>The final decision on revocation of the certificate is left to the Avaya Product Certificate Authority.</p>
Procedure for revocation request	<p>The Avaya Product Certificate Authority accepts revocation requests by email only:</p> <p>apca@avaya.com</p> <p>The email must be authenticated and must include the serial number and subject name of the certificate in question.</p>
Revocation request grace period	Avaya determines a timeframe for response at the time of the request.
2 of 2	

Additional information

- Remote Feature Activation (RFA) website: <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 3rd-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 72
- [Credentials management](#) on page 75
- [Applying profiles for role-based administration](#) on page 76
- [Managing administrative accounts](#) on page 80
- [Administering authentication passwords](#) on page 81

Credentials complexity and expiration requirements

Communication Manager logins comply with:

- [Password complexity policies](#) on page 72
- [Credentials expiration and lockout policies](#) on page 73

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	Customer-defined. Default is 6.
Number of previous passwords that must not match	Customer-defined 0-12. 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 Maintenance Web Interface. 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.


Login Account Policy

This page allows you to establish policies for administrator logins. These policies change future behavior, but do not change existing logins.

Credential Expiration Parameters

The maximum number of days a password may be used (PASS_MAX_DAYS):

The minimum number of days allowed between password changes (PASS_MIN_DAYS):

The number of days a warning is given before a password expires (PASS_WARN_AGE):

The number of days after a password expires to lock the account (INACTIVE; 0 = immediate, 99999 = never):

Passwords

Failed Login Response

☒ Enable account lock out parameters (PAM tally)

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

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

Reset the failed attempt counter after last failed attempt (UNLOCK_RESET): ☒ yes ☐ no

Field	Parameters
Credential Expiration Parameters	
Maximum number of days a password may be used	1-99999
Minimum number of days allowed between password changes	0-99999
Number of days warning given before password expires	0-30
Days after password expires to lock account	0-99999 ¹
Failed Login Response	
Enable account lock out parameters	If not checked, the remaining parameters (below) are ignored.
Lock out login after the following number of unsuccessful attempts	1-9
Automatically unlock a lock account after the following number of seconds	1-99999
Reset the failed attempt counter after last failed attempt	Yes or No

1. 0 = immediate; 99999 = never.

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 1-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 3DES 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 39

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 23](#) lists examples of such profiles.

Table 23: 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 77 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 3: 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

☐ Remove Login

☐ Lock/Unlock Login

☐ Add Group

☐ Remove Group

Submit **Help**

2. Select both the **Add Login** and **Privileged Administrator** buttons then click **Submit**.
The **Administrator Accounts -- Add Login: Privileged Administrator** page displays.

Figure 4: 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:

Additional groups (profile):

Linux shell:

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. Fill in the required fields from [Table 24](#).

Table 24: 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.
Primary group	Set to "susers" and cannot be changed.
Additional groups	Drop-down menu contains profiles 18 (default) through 69.
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)

1 of 2

Table 24: Privileged Administrator field descriptions and values

Field	Description / Values
Date to disable	Enter a date when the login should be disabled in the <i>yyyy-mm-dd</i> format or blank (never disabled).
Type of authentication	<ul style="list-style-type: none"> ● Password ● ASG: enter key ● ASG: Auto-generate key. Selecting this button deactivates the Enter key or password and Re-enter key or password fields.
Enter key or password	<p>Field can be up to 31 characters: a-z, A-Z, 0-9, . (period), - (hyphen), _ (underscore), \$ (dollar sign), blank, : (colon), ' (semi-colon), , (comma), = (equal sign), / (forward slash), & (ampersand), # (pound sign), + (plus sign), ' (apostrophe), * (asterisk), " (quote), ((opening parenthesis), and) (closing parenthesis).</p> <p>The ASG key must be exactly 20 digits (each must be 0-7): the last digit must be "0," and the next-to-the last digit must be even.</p>
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 .
2 of 2	

More information

For information on administering profiles, see:

- http://support.avaya.com/elmodocs2/white_papers/CM_Administrator_Logins.pdf to view and download the *Communication Manager Administrator Logins White Paper*.
- <http://support.avaya.com/japple/css/japple?PAGE=Product&temp.productID=136527> to download the *Documentation for Avaya Communication 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 25: Managing Communication Manager accounts](#) on page 80. See also *Avaya Aura® Communication Manager Feature Description and Implementation (555-245-205)*.

Table 25: Managing Communication Manager accounts

Communication Manager account administration	Interface
Managing Avaya Server web interface login accounts <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 Data Encryption Standard (56-bit DES 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. Assignment of ASG authentication fails if it is not enabled in the server 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 26](#) lists and compares the features of ASG Guard and ASG Guard II.

Table 26: 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](#) on page 84

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 85

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.

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, the firewall configuration, or [Tripwire](#).

Note:

You cannot disable logging of security events.

[Table 27](#) shows the syslog priority and facility for security and non-security events.

Table 27: 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 86
- [Configuring the syslog server in Communication Manager](#) on page 91
- [Accessing system logs through the Web](#) on page 96 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 132 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 87
- [SNMP Agents page](#) on page 87
- [SNMP Traps page](#) on page 89 and [Add Trap Destination page](#) on page 90

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 5](#)).

Figure 5: Agent Status page



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 6](#)).

Note:

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

Figure 6: SNMP Agents page

SNMP Agents

The SNMP Agents Web page allows modification of SNMP properties. SNMP allows the active media 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.

[View G3-AVAYA-MIB Data](#)

Master Agent status: Up

IP Addresses for SNMP Access

☒ No Access
☐ Any IP address
☐ Following IP addresses:
 IP address1 :
 IP address2 :
 IP address3 :
 IP address4 :
 IP address5 :

SNMP Users / Communities

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

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

☐ **Enable SNMP Version 3**

User (read-only)
 User Name :
 Authentication Password : (for authentication and privacy)
 Privacy Password : (for privacy)

User (read-write)
 User Name :
 Authentication Password : (for authentication and privacy)
 Privacy Password : (for privacy)

This page allows you to:

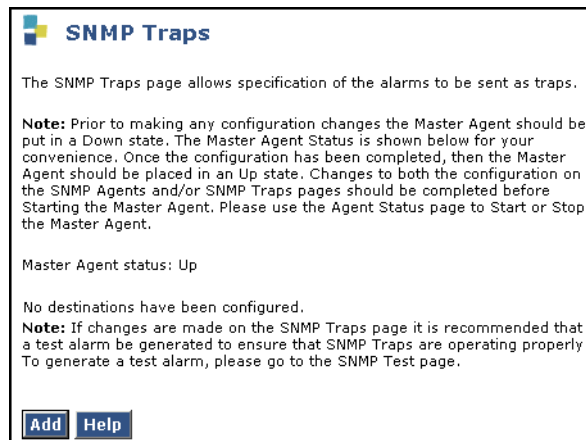
- Block access to the SNMP port
- Monitor the SNMP port for incoming requests and commands (gets and sets) from specified IP address or any IP address

- Enable SNMP v1, v2, or v3

SNMP Traps page

The SNMP Traps page ([Figure 7](#)) allows you to specify which alarms are sent as traps.

Figure 7: SNMP Traps page



Click on the **Add** button to administer alarm traps and their destination(s), as shown in [Figure 8](#).

Figure 8: Add Trap Destination page

Add Trap Destination

Fill-in IP address and provide data for one of the three SNMP versions.

☐ Check to enable this destination.

IP address: . . .

☐ **SNMP version 1**

Community name:

☐ **SNMP version 2c**

Notification type:

Community name:

☐ **SNMP version 3**

Notification type:

User name:

Security Model:

Authentication Password: Must be at least 8 characters

Privacy Password: Must be at least 8 characters

Engine ID:

Add **Help**

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 87 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 92 details what syslog contains, file synchronization options, and firewall activity for the syslog server.
- [Administering the syslog server in Communication Manager](#) on page 92 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 93.

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 2: Logging Levels form, page 1](#) on page 94).
- 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 1](#)).

Figure 1: Syslog Server Web page

This 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 2](#)) 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 2: Logging Levels form, page 1

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	

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 3](#)) allows further refinement of the information that is delivered to the syslog.

Figure 3: Logging Levels form, page 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	

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
1 of 2		

Field	Values	Description
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.
2 of 2		

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 9](#)). 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 9: 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.

Select Log Types (multiple log output will be merged)

- ☐ Logmanager debug trace
- ☐ Operating system boot messages
- ☐ Linux scheduled task log (CRON)
- ☐ Linux kernel debug messages
- ☐ 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
- ☐ System updates/patches

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
- ☐ 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

Select Event Range

☒ Today

☐ Yesterday

☐ view entries for this date and time: (mm:dd:yyyy) (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: ☐ Newest First ☐ Remove Header

More information

- [Restricting Web access to system logs](#) on page 132
- [Reading and interpreting the security logs](#) on page 133

Chapter 3: Network Security Integration

Firewall/topology configurations

- [Administering firewall settings in Communication Manager](#) on page 97

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 28](#) lists the Communication Manager firewall default settings:

Table 28: 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
1 of 3			

Table 28: Default Communication Manager firewall settings

Input to server	Output from server	Service	Port/protocol
	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
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
2 of 3			

Table 28: Default Communication Manager firewall settings

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

Network "best practices"

- [Separation of network functionality](#) on page 100
- [Layer 2 and Layer 3 hardening](#) on page 101
- [Designing VLAN groups for functional network segmentation](#) on page 110
- [How ARP spoofing facilitates network attacks](#) on page 112
- [Security strategies to combat ARP spoofing](#) on page 113
- [Security vulnerabilities with name and address management](#) on page 113
- [How Communication Manager addresses NIST recommendations](#) on page 116
- [Recommendations for preventing DoS attacks](#) on page 121

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 the Tripwire feature (see [Tripwire](#) on page 35) and other logging capabilities (see [Configuring SNMP and syslog](#) on page 85), 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 than 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*.

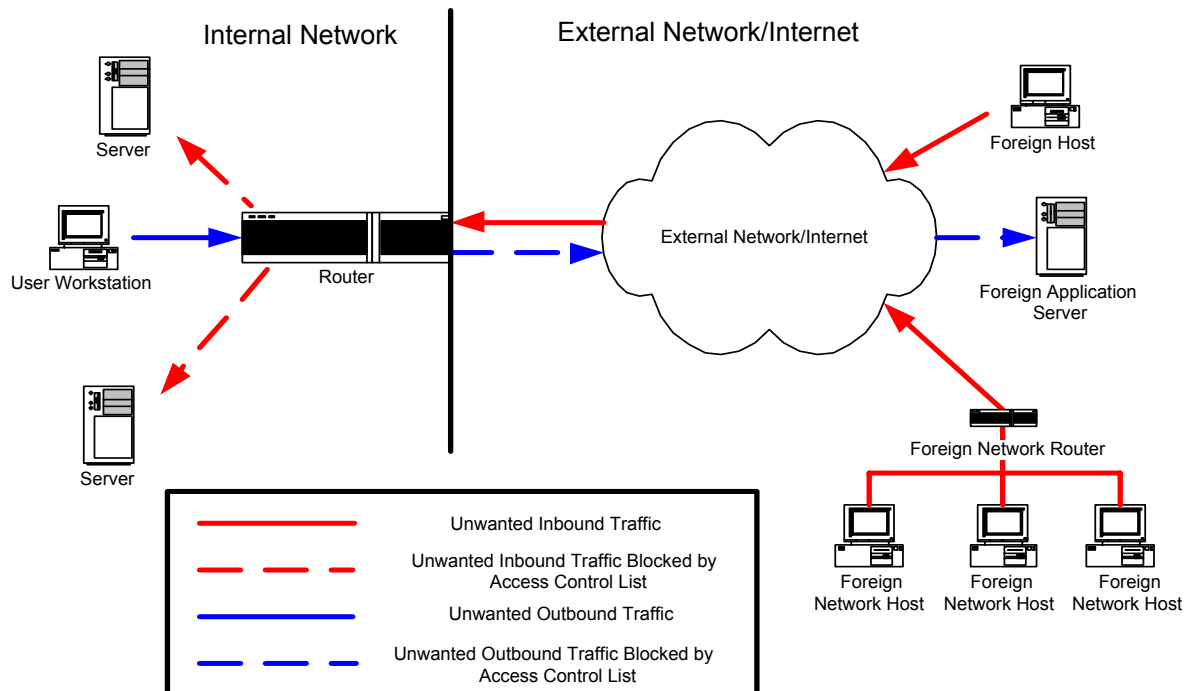
Access control lists

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 10: Network Security using access control lists](#) on page 104 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 10: Network Security using access control lists



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 106
- [External authentication accounts](#) on page 106
- [External authentication servers](#) on page 107

External authentication accounts

External authentication account server requirements are listed in [Table 29: External Authentication Accounts](#).

Table 29: External Authentication Accounts

External authentication accounts	Required external servers	Authentication information
LDAP - based accounts	<p>Require an LDAP server compatible with the LDAP client from www.openldap.org.</p> <p>LDAP servers tested with Communication Manager are:</p> <ul style="list-style-type: none"> • The server from www.openldap.org • Microsoft Active Directory • SunOne Directory Service 	<p>The LDAP module that resides on the Avaya Server authenticates with an external LDAP server.</p> <p>When logins are configured at OpenLDAP:</p> <ul style="list-style-type: none"> • Avaya Services logins are authenticated locally (Communication Manager) • Customer logins are authenticated either locally or on the LDAP server
RADIUS - based accounts	<p>Require:</p> <ul style="list-style-type: none"> • a RADIUS server compatible with the client from www.freeradius.org • a parallel local host account or an LDAP account for authorization information 	<p>When logins are configured through Communication Manager/RADIUS:</p> <ul style="list-style-type: none"> • Avaya Services logins are authenticated locally (Communication Manager) • Customer logins are authenticated at RADIUS and authorized locally (Communication Manager)
<p>Token - based accounts</p> <ul style="list-style-type: none"> • RSA SecurID • Secure Computing SafeWord 	<ul style="list-style-type: none"> • RSA SecurID (provides only user authentication) or • Secure Computing SafeWord (provides only user authentication) <p>Require a parallel host account or an LDAP account for authorization information.</p>	<ul style="list-style-type: none"> • 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

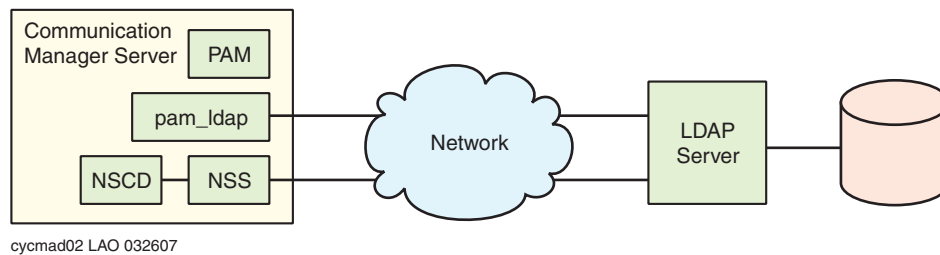
At a minimum, Avaya supports only customer-provided Open LDAP and RADIUS servers on Avaya servers, gateways, and any application that offers user or administrative access and authentication. Communication Manager also supports SafeWord and SecurID for external authentication. Avaya supports no other 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 11](#). Login requires an entry in LDAP only.

Figure 11: LDAP server authentication configuration



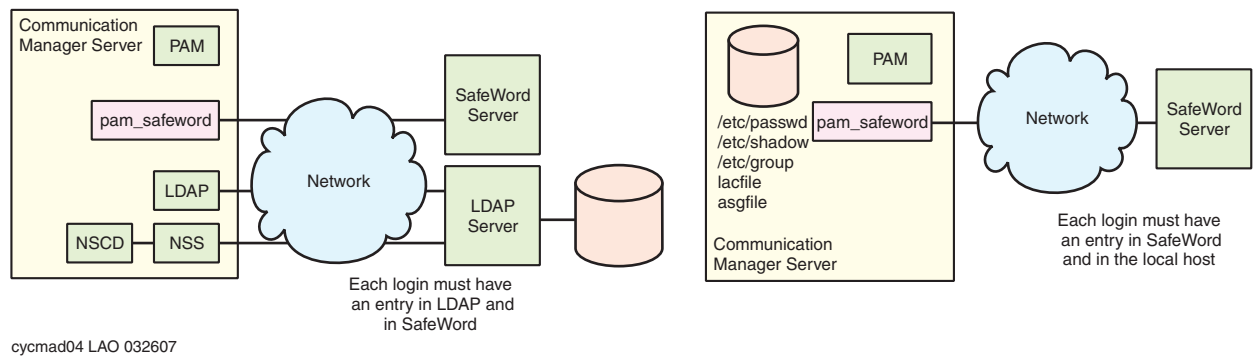
RADIUS servers

External RADIUS provides only user authentication and accounting as shown in [Figure 12: RADIUS server authentication configurations](#) on page 108.

Note:

Communication Manager Branch Gateways support only RADIUS servers.

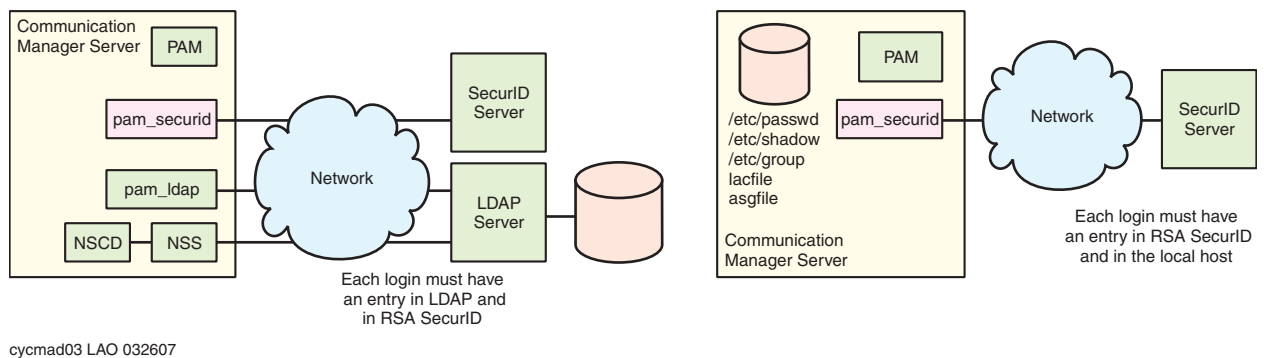
Figure 12: RADIUS server authentication configurations



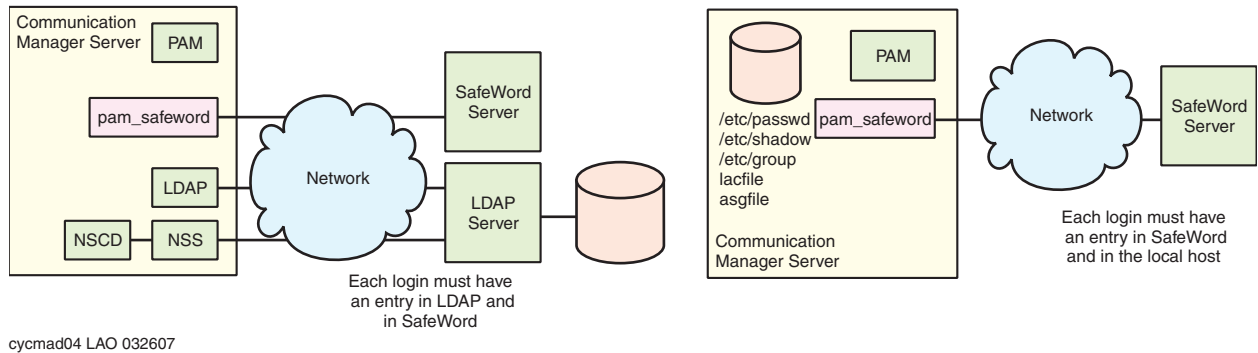
Token servers

RSA SecurID is a token-based authentication method from RSA Security that provides only user authentication. [Figure 13: RSA SecurID server authentication configurations](#) shows configurations with an LDAP server and with a local host (no LDAP server).

Figure 13: RSA SecurID server authentication configurations

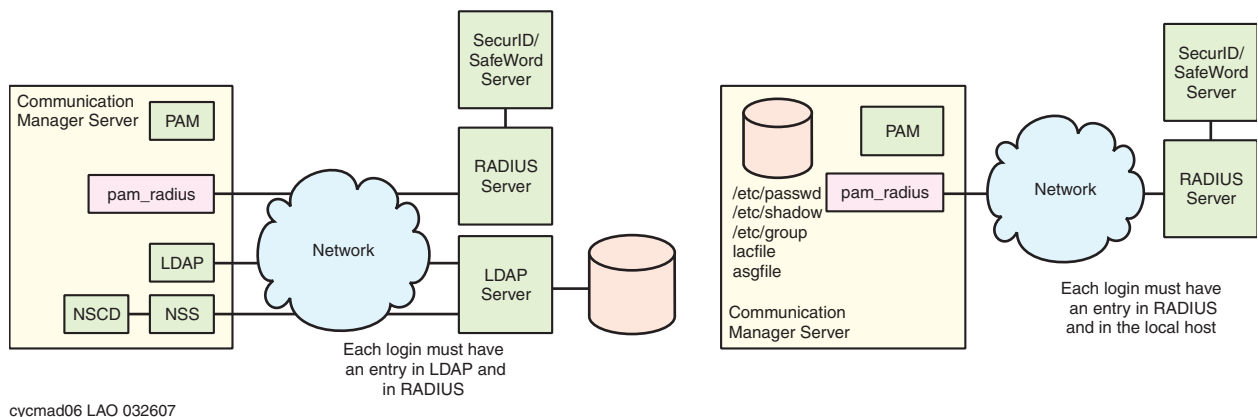


Secure Computing SafeWord is a token-based authentication method from RSA Security that provides only user authentication. [Figure 14: SafeWord server authentication configurations](#) shows configurations with an LDAP server and with a local host (no LDAP server).

Figure 14: SafeWord server authentication configurations

RADIUS plus token servers

[Figure 15: Radius plus token authentication configurations](#) shows an example of another authentication configuration: RSA SecurID and SafeWord used behind an external RADIUS server.

Figure 15: 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 website 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 vice 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 known 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 117
- [Classical wiretap vulnerability](#) on page 117

- [ARP cache poisoning and ARP floods](#) on page 117
- [Web server interfaces](#) on page 118
- [IP phone subnet mask vulnerability](#) on page 118
- [Extension to IP address mapping vulnerability](#) on page 118

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 Gateways*, 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 113.

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 164.

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:
 - ¶ Disclosing confidential data
 - ¶ Causing service deterioration by modifying the system software
 - ¶ Crashing the system
 - ¶ 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:
 - ¶ 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.)
 - ¶ 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 114.

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 164.

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 113.

Default password vulnerability

See [Switch default password vulnerability](#) on page 117.

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 16: 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 30](#) to administer the **Restrict Calls** field on the **Feature-Related System Parameters** form in Communication Manager.

Table 30: 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 31](#) to alert you of security-related events, including DoS conditions.

Table 31: 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 .
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 <i>between</i> traps.

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 32](#) to avoid DoS vulnerabilities from incomplete SIP or H.323 signaling group administration on the Signaling Group form

Table 32: 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	If this field is blank, the system warns you that an unspecified far-end IP address is vulnerable to DoS attacks.
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 138

Chapter 4: Operational Security

Avaya Security Advisories

- [What is an Avaya Security Advisory](#) on page 127
- [How do I get Avaya Security Advisories?](#) on page 128
- [How to interpret an Avaya Security Advisory](#) on page 129

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 129). 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 3rd-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 the following table:

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 step 11.
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 33](#) summarizes the three main categories.

Table 33: Avaya's security vulnerability classification

Vulnerability classification	Criteria for classification
High	<p>The product is vulnerable to:</p> <ul style="list-style-type: none"> ● Attacks from a remote unauthenticated user who: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - Can easily cause the system or a critical application to shutdown, reboot, or become unusable without requiring interaction with a product user. <p>For example, see the advisory at http://support.avaya.com/elmodocs2/security/ASA-2006-002.htm.</p>
Medium	<p>The product does not meet criteria for high vulnerability, but is vulnerable to:</p> <ul style="list-style-type: none"> ● 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. <p>For example, see the advisory at http://support.avaya.com/elmodocs2/security/ASA-2006-262.htm</p>
1 of 2	

Table 33: Avaya's security vulnerability classification

Vulnerability classification	Criteria for classification
Low	<p>The product does not meet criteria for medium or high vulnerability, but is vulnerable to:</p> <ul style="list-style-type: none"> ● 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. <p>For example, see the advisory at http://support.avaya.com/elmodocs2/security/ASA-2007-015.htm.</p>
None	<p>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.</p> <p>For example, see the advisory at http://support.avaya.com/elmodocs2/security/ASA-2006-261.htm.</p>
2 of 2	

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 3rd-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](#) on page 132
- [Restricting Web access to system logs](#) on page 132
- [Where is security information logged?](#) on page 132
- [Reading and interpreting the security logs](#) on page 133

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 26 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 85)
- Syslog security log (see [Configuring the syslog server in Communication Manager](#) on page 91)
- Miscellaneous logs (viewed from the Systems Log page, [Figure 9: System Logs page](#) on page 97) 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](#) on page 133
- [Interpreting SNMP entries in the syslog](#) on page 134
- [Interpreting the platform command history log](#) on page 135
- [Interpreting Communication Manager security violations](#) on page 136
- [Interpreting the command history log for Communication Manager SAT](#) on page 139
- [Interpreting the command history log for Web activity](#) on page 141

Interpreting the syslog header

Each syslog entry has a common header format:

```
yyyymmdd:hh:mm:ssss text
```

Variable	Description
yyyy	The year
mm	The month of the year
dd	The day of the month
hh:mm:ssss	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

```
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
```

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: <ul style="list-style-type: none"> • 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"

Log entry	Description
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
```

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	<p>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:</p> <ul style="list-style-type: none"> • Interpreting the command history log for Communication Manager SAT on page 139 • Interpreting the command history log for Web activity on page 141

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 122).

Action/Object	Qualifier	Qualifier Description	Logins
<code>monitor security-violations</code>	<code>authorization-code</code> <code>remote-access</code> <code>station-security-codes</code>	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 138.

```
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 34: 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
Ext	Extension number through which the security violation occurred
Port/Ext	The type of port and extension through which the security violation occurred
1 of 2	

Table 34: Security Violations Status field descriptions 2 of 2

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 1](#) 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 93.

Table 1: 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
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
1 of 2	

Table 1: Communication Manager SAT command history log format

Field	Description
R	The status of the action: <ul style="list-style-type: none"> ● 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

- 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.

**SECURITY ALERT:**

Authorization codes, PINs, encryption keys, and passwords never appear in the command history log.

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 2](#) lists and describes the text formats in the log entry for Web activity.

Table 2: 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
1 of 2	

Table 2: Abbreviated Dialing Button Programming command history log format

Field	Description
R	The status of the action: <ul style="list-style-type: none"> ● 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
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 1](#) (the page as it is initially presented to the user).

Figure 1: Backup Now page with initial defaults

Backup Now

The Backup Now Web page lets you store data separate from the Avaya media server. Select the type of data and the method to backup. Encrypting the data while backing up provides you a high level of security and is strongly encouraged.

Data Sets

☒ Specify Data Sets

☒ Avaya Call Processing (ACP) Translations

☒ Save ACP translations prior to backup

☐ Do NOT save ACP translations prior to backup

☐ Server and System Files

☐ Security Files

☐ Full Backup

Note: A CM "save trans" is not executed by the Full Backup

Backup Method

☐ Network Device

Method:

User Name:

Password:

Host Name:

Directory:

☐ Local CompactFlash Card Retain data sets at destination

☐ Format CompactFlash

Encryption


☐ Encrypt backup using pass phrase

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

Now the page appears as shown in [Figure 2: Backup Now page after user changes](#) on page 144.

Figure 2: Backup Now page after user changes

 **Backup Now**

The Backup Now Web page lets you store data separate from the Avaya media server. Select the type of data and the method to backup. Encrypting the data while backing up provides you a high level of security and is strongly encouraged.

Data Sets

☒ Specify Data Sets

☐ Avaya Call Processing (ACP) Translations

☒ Save ACP translations prior to backup

☐ Do NOT save ACP translations prior to backup

☐ Server and System Files

☒ Security Files

☐ Full Backup

Note: A CM "save trans" is not executed by the Full Backup

Backup Method

☒ Network Device

Method

User Name

Password

Host Name

Directory

☐ Local CompactFlash Card Retain data sets at destination

☐ Format CompactFlash

Encryption

☐ Encrypt backup using pass phrase

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/Firmware updates

- [How Avaya delivers security updates](#) on page 146
- [Applying an operating system security update](#) on page 148
- [Applying an Avaya field load or software update](#) on page 148

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:

Vulnerability	Target remediation intervals
High	<p>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).</p> <p>If a software patch is available for installation or another action is recommended, the Avaya Security Advisory describes the actions.</p>
Medium	<p>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).</p> <p>If a software patch is available for installation or another action is recommended, the Avaya Security Advisory describes the actions.</p>
Low	<p>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).</p> <p>If a software patch is available for installation or another action is recommended, the Avaya Security Advisory describes the actions.</p>
None	No remediation actions are required.

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 150
- [Considerations for customers who must comply with the Graham-Leach-Bliley Act](#) on page 152
- [Considerations for customers who must comply with HIPAA](#) on page 154
- [Considerations for customers who must comply with CALEA](#) on page 155
- [Considerations for customers who must comply with FISMA](#) on page 156
- [Considerations for customers who want to comply with ISO 17799](#) on page 157
- [Considerations for customers who must comply with E911](#) on page 160
- [Considerations for non-US customers who must comply with regulations](#) on page 162

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.

Features related to data security and documented in more detail in other sections of this document are:

Feature	How related to Sarbanes-Oxley	Where documented
Encryption	Transmitted data is protected from packet-sniffing and eavesdropping	See: <ul style="list-style-type: none"> • Avaya's encryption overview on page 39
Access control	Access to data is protected from unauthorized personnel	See: <ul style="list-style-type: none"> • Access profiles on page 25 • Managing administrative accounts on page 80
Authentication	Access to the system is restricted by login/password.	See: <ul style="list-style-type: none"> • Access profiles on page 25 • Managing administrative accounts on page 80
1 of 2		

Feature	How related to Sarbanes-Oxley	Where documented
Logging	Security-related events are logged	See: <ul style="list-style-type: none"> • Configuring SNMP and syslog on page 85 • Reading and interpreting the security logs on page 133
Backup of data	Data saved on backup media or backup server. Protected by encryption and key.	See: <ul style="list-style-type: none"> • Secure backups of Communication Manager data and translations on page 164
2 of 2		

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.

Feature	How related to Graham-Leach Bliley Act	Where documented
Encryption	Transmitted and stored data is protected from unauthorized individuals.	See: <ul style="list-style-type: none">• Avaya's encryption overview on page 39
System access control	Access to data is protected from unauthorized personnel.	See: <ul style="list-style-type: none">• Access profiles on page 25• Managing administrative accounts on page 80
Authentication	Access to the system is restricted by login/password.	<ul style="list-style-type: none">• Access profiles on page 25• Managing administrative accounts on page 80
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 <ul style="list-style-type: none">• Secure backups of Communication Manager data and translations on page 164

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.

Feature	How related to HIPAA	Where documented
Encryption	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate	See: <ul style="list-style-type: none">• Avaya's encryption overview on page 39
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: <ul style="list-style-type: none">• Managing administrative accounts on page 80
Authentication	Implement procedures to verify that a person or entity seeking access to electronically-protected health information is the one claimed.	See: <ul style="list-style-type: none">• Access profiles on page 25• Managing administrative accounts on page 80
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: <ul style="list-style-type: none">• Managing administrative accounts on page 80

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:

Feature	How related to FISMA	Where documented
Encryption	Transmitted data is protected from packet-sniffing and eavesdropping and other unauthorized access.	See: <ul style="list-style-type: none">• Avaya's encryption overview on page 39
System access control	Access to data is protected from unauthorized personnel	See: <ul style="list-style-type: none">• Managing administrative accounts on page 80
Authentication	Access to the system is restricted by login/password.	See: <ul style="list-style-type: none">• Administering authentication passwords on page 81

1 of 2

Feature	How related to FISMA	Where documented
Logging	Security-related events are logged	See: <ul style="list-style-type: none"> • Configuring SNMP and syslog on page 85 • Reading and interpreting the security logs on page 133
Firewall	Access to Communication Manager network is protected	See: <ul style="list-style-type: none"> • Firewall protection on page 18
Backup of data	Data saved on backup media or backup server. Protected by encryption and key	See <ul style="list-style-type: none"> • Secure backups of Communication Manager data and translations on page 164
Toll fraud prevention	Unauthorized use of long-distance is prevented	See <ul style="list-style-type: none"> • Limiting long-distance access on page 84
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.

ISO 17799 addresses the following broad categories of data security management:

ISO 17799 Security Guidelines	Communication Manager features and processes
Ensure that applications process information correctly	
<ul style="list-style-type: none"> ● Use validation checks to control processing 	<p>Use the System Log and Maintenance Alarm and Event logs. See:</p> <ul style="list-style-type: none"> ● Configuring SNMP and syslog on page 85 ● Reading and interpreting the security logs on page 133
<ul style="list-style-type: none"> ● Validate data input into your applications 	<p>Communication Manager can track administration and notify the administrator when changes are made. Use Tripwire, the System Log, and the Maintenance Alarm and Event logs. See:</p> <ul style="list-style-type: none"> ● Tripwire on page 35 ● Configuring SNMP and syslog on page 85 ● Reading and interpreting the security logs on page 133 ● <i>Maintenance Procedures for Avaya Aura® Communication Manager, Media Gateways and Servers (03-300432)</i> ● <i>Maintenance Commands for Avaya Aura® Communication Manager, Media Gateways and Servers (03-300431)</i>
<ul style="list-style-type: none"> ● Protect message integrity and authenticity 	<p>Use digital certificates when transmitting data to ensure authorization. Restrict access to the system with logins, passwords, and authentication keys. See:</p> <ul style="list-style-type: none"> ● Chain of trust on page 62 ● Administering authentication passwords on page 81
<ul style="list-style-type: none"> ● Validate your applications' output data 	<p>Use audits and status reports to verify output. See:</p> <ul style="list-style-type: none"> ● <i>Maintenance Procedures for Avaya Aura® Communication Manager, Media Gateways and Servers (03-300432)</i> ● <i>Maintenance Commands for Avaya Aura® Communication Manager, Media Gateways and Servers (03-300431)</i>
1 of 3	

ISO 17799 Security Guidelines	Communication Manager features and processes
<ul style="list-style-type: none"> ● Use cryptographic controls to protect your information 	<p>Encrypt data to protect data from packet-sniffing and eavesdropping.</p> <p>See:</p> <ul style="list-style-type: none"> ● Avaya's encryption overview on page 39 ● Secure updates of Avaya software and firmware on page 164
Protect and control your organization's system files	
<ul style="list-style-type: none"> ● Control the installation of operational software 	<p>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.</p> <p>See</p> <ul style="list-style-type: none"> ● Security problems addressed by digital certificates on page 24 ● Secure updates of Avaya software and firmware on page 164
<ul style="list-style-type: none"> ● Control the use of system data for testing 	<p>Avaya uses internal ISO-certified testing processes for software.</p>
<ul style="list-style-type: none"> ● Control access to program source code 	<p>Communication Manager source code is not accessible outside of Avaya. The Red Hat Linux operating system is also restricted.</p> <p>See</p> <ul style="list-style-type: none"> ● Why Avaya chose the Linux operating system for Communication Manager on page 17
Control development and support processes	
<ul style="list-style-type: none"> ● Establish formal change control procedures 	<p>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 146.</p>
<ul style="list-style-type: none"> ● Review applications after operating system changes 	<p>Avaya uses internal ISO-certified test procedures after operating system changes. See Validating a security update on page 147.</p>
<ul style="list-style-type: none"> ● Restrict changes to software packages 	<p>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.</p>
2 of 3	

ISO 17799 Security Guidelines	Communication Manager features and processes
<ul style="list-style-type: none"> ● Prevent information leakage 	Communication Manager does not have antivirus, antiworm, or antitrojan software. However, Avaya does not recommend using 3rd party antivirus software on Communication Manager. For more information, see Planning against viruses and worms and other malicious code on page 20.
<ul style="list-style-type: none"> ● Control outsourced software development 	Avaya software, if outsourced, is developed according to Avaya's ISO-certified processes.
Control your technical system vulnerabilities	<p>Communication Manager offers many features and processes to protect the customer's communications network. See:</p> <ul style="list-style-type: none"> ● Avaya's encryption overview on page 39 ● Managing administrative accounts on page 80 ● Configuring SNMP and syslog on page 85 ● Chain of trust on page 62 ● Avaya Public Key Infrastructure on page 63 ● Configuring SNMP and syslog on page 85 ● Secure backups of Communication Manager data and translations on page 164 ● Secure updates of Avaya software and firmware on page 164
3 of 3	

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® 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 backup/download

- [Secure backups of Communication Manager data and translations](#) on page 164
- [Secure updates of Avaya software and firmware](#) on page 164

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 SystemsSM 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 VPNNet 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: Physical Interfaces and Associated Network Services

Communication Manager runs on four Linux-based servers:

- [Avaya S8300 Server](#)
- [Avaya S8400 Server](#)
- [Avaya S8500 Series Servers](#)
- [Avaya S8700 Series Servers](#)

Each server has similar, but uniquely designed, interfaces over which [Network Services on Communication Manager Servers](#) communicate.

Avaya S8300 Server

An S8300 Media Server (version C) is an Intel Celeron-based processor that runs the Linux operating system. The S8300 Media Server resides in Slot V1 of a G700 Media Gateway and includes:

- A 60-GB hard disk
- 1 GB RAM (with one 1 GB DIMM)
- 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 that is used as the primary reboot device and provides additional reliability with the RAMdisk and hard drive.

The S8300 Media Server resides in a media gateway, and specifically in Slot V1 of a G700 Media Gateway as show in [Figure 17: S8300 Media Server in a G700 Media Gateway \(S8300C shown\)](#) on page 168. The G700 is architecturally based on the Avaya P330 and C360 switches and contains VoIP resources and modular interface connectivity. The media modules provide analog, digital, T1/E1, BRI, and additional VoIP capabilities.

TN8300C access / connectivity

[Figure 17](#) shows access to critical components of the media server or to its connection ports.

Figure 17: S8300 Media Server in a G700 Media Gateway (S8300C shown)

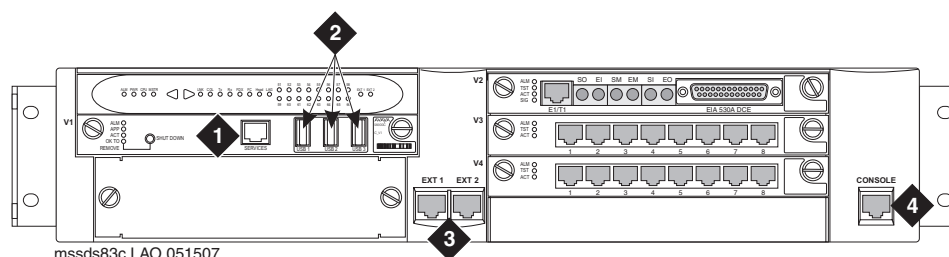


Figure notes:

- | | |
|------------------|--|
| 1. Services port | 3. Dual 10/100 Base-T Ethernet switch ports |
| 2. USB ports | 4. Console connection for on-site administration |

Avaya S8400 Server

S8400 Media Server is a TN circuit pack that resides in a port network cabinet (for example, G650) and is composed of the:

- TN8400AP Media Server circuit pack (see [Figure 18: Avaya TN8400AP \(interior\)](#) on page 169 and [Figure 19: Avaya TN8400AP \(front\)](#) on page 171)
- TN8412AP S8400 IP Interface (SIPI) circuit pack (see [Figure 20: Avaya TN8412 \(SIPI\) circuit pack](#) on page 172)
- Optional media server cable adapter (see [Figure 21: Media server cable adapter \(mounted on rear of TN8400AP\)](#) on page 174)

Communication between the S8400 Media Server and the TN8412AP is by IP link connected by an external switch or point-to-point by a single Ethernet crossover cable. The TN8412AP has a single Ethernet interface for control.

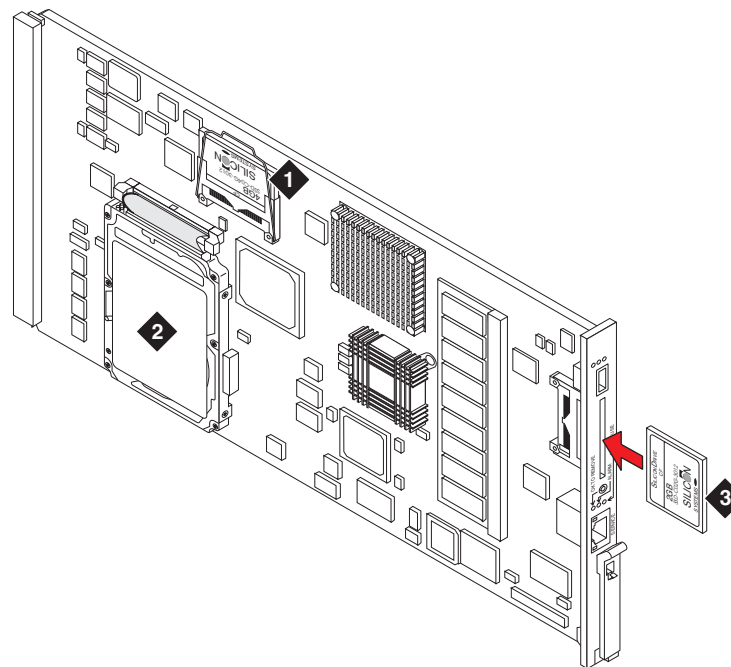
TN8400AP access / connectivity

The following figures show access to critical components of the media server or to its connection ports:

- [Figure 18: Avaya TN8400AP \(interior\)](#) on page 169
- [Figure 19: Avaya TN8400AP \(front\)](#) on page 171
- [Figure 20: Avaya TN8412 \(SIPI\) circuit pack](#) on page 172
- [Figure 21: Media server cable adapter \(mounted on rear of TN8400AP\)](#) on page 174

TN8400AP circuit pack

Figure 18: Avaya TN8400AP (interior)



h2sd8400 LAO 051507

Figure notes:

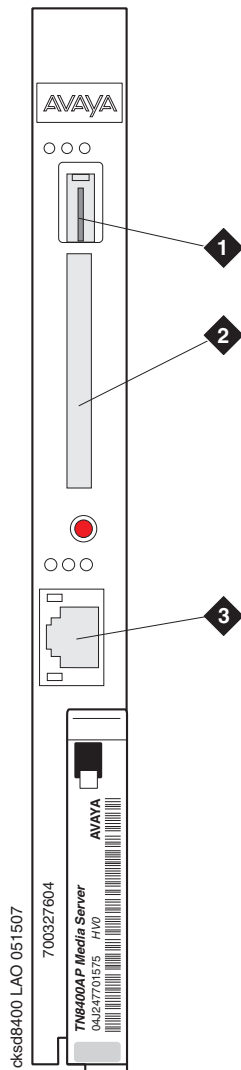
- | | |
|--|--|
| 1. Solid state drive (SSD) contains Linux OS and Communication Manager files | 3. Compact Flash contains Communication Manager translations |
| 2. Hard disk drive stores voice messages | |
-

The S8400 Media Server uses a solid state drive (SSD) and a hard disk drive (HDD) to:

- Run Communication Manager (SSD and HDD)
- Hold translations (Compact Flash only; the SSD does not store translations)

The SSD and CD/DVD-ROM drive each can be configured as a bootable device.

Critical Communication Manager application files and translations are loaded onto the SSD. This means that in the event of a hard disk drive failure, many critical functions are still available, and the S8400 Media Server will come back into service if the server is rebooted.

Figure 19: Avaya TN8400AP (front)**Figure notes:**

- | | | | |
|----|---------------------------|----|-----------------------------------|
| 1. | USB port for CD-ROM drive | 3. | Ethernet port for Services laptop |
| 2. | Compact Flash slot | | |
-

TN8412 (SIPI) circuit pack

Figure 20: Avaya TN8412 (SIPI) circuit pack

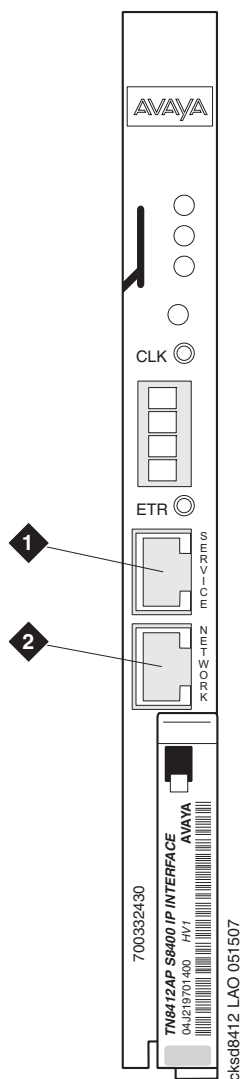


Figure notes:

- | | |
|--------------------------|------------------------|
| 1. Ethernet Service port | 2. Ethernet to Network |
|--------------------------|------------------------|

The S8400 Media Server uses the TN8412AP S8400 IP Interface (SIPI) circuit pack to provide:

- Circuit pack control within its port network
- Cabinet maintenance
- Tone-clocks
- Emergency transfer switch functionality

- Customer/external alarms

The physical connection between the TN8412AP/TN2312BP and the S8400 circuit packs is made by either:

- Using an external crossover cable that directly interconnects the appropriate backplane pins of the two circuit packs. The interface between the TN8400AP and the TN8412AP is by a 10/100 Base T Ethernet crossover cable on the backplane connector. An RJ45 cable, that plugs into the TN8400AP media server cable adapter ETH-A port and the TN8412APIPSI-2 adapter control port, provides the direct connection between the TN8400AP and the TN8412AP.
- Through the customer LAN connection

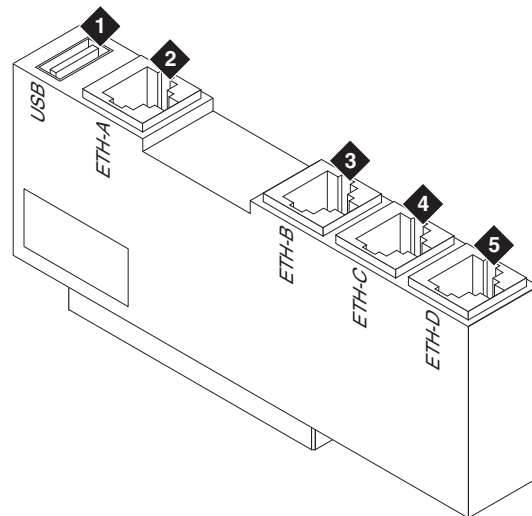
The SIPI can be accessed remotely using the TELNET and SSH protocols. The SIPI can serve as an SSH client, as well, for remote access from the SIPI to the Communication Manager server. The C-LAN can also serve as an FTP or SFTP server for file transfers — primarily firmware downloads.

Note:

The SIPI cannot serve as an SFTP client. Additionally, the SSH/SFTP capability is only for the control network interface, not the Services interface.

S8400 cable adapter

Figure 21: Media server cable adapter (mounted on rear of TN8400AP)



addp84bk LAO 112905

Figure notes:

- | | |
|-------------------------------------|-----------------------------|
| 1. USB modem connector ¹ | 4. Ethernet connector ETH-C |
| 2. Ethernet connector ETH-A | 5. Ethernet connector ETH-D |
| 3. Ethernet connector ETH-B | |
1. Provides Avaya Services with remote alarming and dial-in and dial-out access. The modem communicates directly to the maintenance processor or tunnels through to the Communication Manager application.
-

[Table 35](#) describes the connections for the media server cable adapter.

Table 35: Media server cable adapter port labeling

Location (counting from the top of the adapter)	Port Name	Adapter Label	Function
USB	Backplane USB modem port	USB	Provides power to the USB modem, can hard reset the USB modem, provides a USB modem interface to support Services remote alarming and access.
Top Ethernet	Ethernet connectivity with the TN8412AP circuit pack	ETH-A	10/100Base T Ethernet Interface for the control links - uses crossover cable to connect directly to the SIPI.
Second Ethernet	Ethernet connectivity with the TN2302BP circuit pack	ETH-B	10/100Base T Ethernet Interface for Messaging over IP - connects to the customer LAN.
Third Ethernet	Future	ETH-C	Not used
Bottom Ethernet	Future	ETH-D	Not used

Avaya S8500 Series Servers

The Avaya S8500 Series Server is a rack mounted telephony server. The S8500 runs the Linux operating System, and features Communication Manager. The S8500 can support Internet Protocol (IP), Session Initiation Protocol (SIP), and traditional endpoints.

S8500 access / connectivity

The following figures show access to critical components of the media server or to its connection ports:

- [Figure 22: S8500C Media Server \(front\)](#) on page 176
- [Figure 23: S8500C Media Server \(back\)](#) on page 176

Figure 22: S8500C Media Server (front)

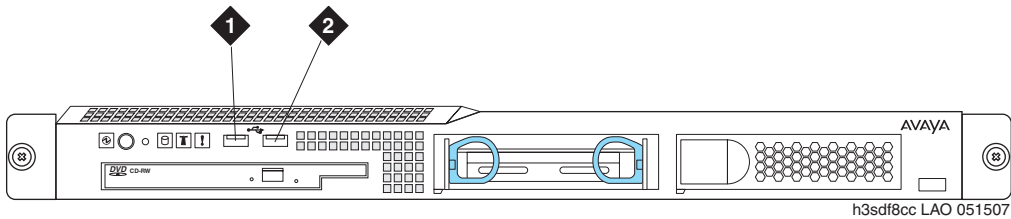


Figure notes:

- | | |
|-------------|-------------|
| 1. USB port | 2. USB port |
|-------------|-------------|

Figure 23: S8500C Media Server (back)

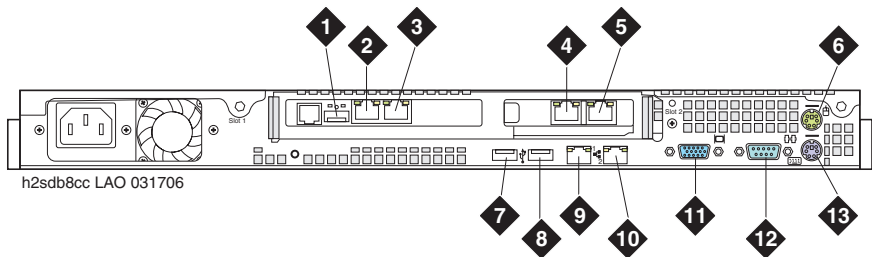


Figure notes:

- | | |
|----------------------------------|-----------------------------------|
| 1. USB connection (to USB modem) | 8. USB port |
| 2. SAMP Ethernet (not used) | 9. Ethernet 1 |
| 3. SAMP services port | 10. Ethernet 2 |
| 4. Ethernet 4 | 11. Video connector |
| 5. Ethernet 3 | 12. Serial connector |
| 6. Mouse connector (not used) | 13. Keyboard connector (not used) |
| 7. USB port | |

The S8500C server connections include:

- Two USB ports on the front and two USB ports on the back. One of the four ports is used for the [Compact Flash](#) drive.

Note:

The SAMP card also has one USB port that is *in addition to* the four specified on the S8500C itself (See [Server Availability Management Processor \(SAMP\)](#) on page 177). The [Compact Flash](#) memory reader is always connected to a USB port on the S8500C chassis, *not* on the SAMP card.

- One serial port can be used for console redirection
- A keyboard port (not used)
- A mouse port (not used)
- Two 10/100/1000Base-T Ethernet ports
- A [Server Availability Management Processor \(SAMP\)](#) card for maintenance
- An external Compact Flash Memory Reader
- A [Compact Flash](#) 128 MB industry media (optional)
- One USB modem that connects to the USB port on the SAMP. The modem provides remote access to:
 - O/S and environmental alarms through port 10022
 - Communication Manager alarms through port 22
- Dual-NIC card

Server Availability Management Processor (SAMP)

The SAMP card is a remote maintenance and serviceability card that is pre-installed in the S8500C Media Server.

The SAMP card:

- Monitors the server state of health: fans, voltages, and temperature
- Reports server failure and other alarms to INADS by modem
- Provides remote server power-on and reset capability
- Provides secure dial-in connection to the SAMP, and subsequently the host, using SSH, secure shell
- Provides Services laptop access to the SAMP, and subsequently the host

Power to the SAMP is derived from an external power source. This power source uses its own built-in transformer or receives power from the S8500C Media Server through its connection at the PCI bus. Avaya recommends that an external power source on a different circuit from the S8500C be provided for the SAMP. In this way, if the SAMP's power fails, the S8500C can provide backup power.

Compact Flash

You can backup the S8500 Media Server to a server on the LAN or to the Compact Flash memory reader. This reader is installed in one of the USB ports. The Compact Flash memory reader uses a 128-MB Compact Flash card. Avaya recommends use of the industrial grade Compact Flash card for the following reasons:

- Improved data integrity and reliability
 - Powerful error correction
- Extreme endurance
 - 2,000,000 program/erase cycles per block
- Increased reliability
 - Mean time between failures (MTBF) greater than 3 million hours
- Industry-leading 7-year warranty
- Enhanced durability
 - New RTV silicone for added strength and stability

The industrial grade Compact Flash is available through Avaya and Avaya business partners.

S8510 access / connectivity

The Avaya S8510 Server uses a Dell™ PowerEdge™ 1950 System configured with:

- One Quad Core Intel® Xeon® E5410 Processor 5000 Sequence
- Optional dual hard disk drives with RAID (Redundant Array of Independent Disks) Level 1 that provides disk mirroring (identical data on both disks that can work independently) to increase the system reliability.
- One hot-pluggable, 670-W power supply with an option of installing a second, backup power supply
- Dual NIC
- [Server Availability Management Processor](#) (Augmentix A+SAMP™) card for remote maintenance and serviceability of the server
- [Modem](#) connection through the A+SAMP™ USB port that is shared between the HOST server and the A+SAMP™ card for remote maintenance, administration, and alarming.
- Embedded Avaya Voice Messaging application co-resident with Communication Manager.
- The SIP Enablement Services (SES) application is also offered co-resident with Communication Manager.

Server Availability Management Processor

The Server Availability Management Processor (SAMP) is a remote maintenance board that monitors and reports alerts from components within the S8510 Server. The SAMP is pre-installed on the S8510 server for products that use it.

The SAMP board:

- Monitors the server boot process, the Communication Manager watch dog, the fans, the voltages, and the temperature.
- Reports server failure alarms and other alarms to INADS or other services group by modem.
- Provides remote server power-on and reset capability
- Provides secure dial-in connection to the SAMP, and subsequently the server, using SSH, secure shell.
- Provides Services access to the SAMP, and subsequently the server.

The SAMP board is a half-card form factor installed in the PCI-e expansion slot on the Avaya S8510 server and is powered externally. The SAMP supports

- Two Ethernet ports:
 - Ethernet 1 (Eth1) is not used.
 - Ethernet 2 (Eth2) is the Avaya Services port for direct access to the SAMP
- One USB port for the USB modem for remote dial-in access. A user first establishes a Point-to-Point Protocol (PPP) session that terminates at the SAMP. The user then establishes an SSH (Secure Shell) or an HTTPS (Secure Web) session to the SAMP or to the server itself.

The SAMP also communicates with the host in-band through an on-board, industry-standard Ethernet controller on the host's PCI bus with an internal link to the SAMP.

For information on installing software on the SAMP and changing the default settings see *Server Availability Management Processor: Avaya S8510 Server, 03-602923*.

Modem

The modem provides remote access to the server when the customer has a maintenance contract with Avaya. Operating system and environmental alarms are sent through the modem to INADS or other service provider. Maintenance technicians can dial into the server through the modem.

If the S8510 server is equipped with the SAMP remote maintenance board, the modem connects to the USB port on the SAMP. If the S8510 server does not have a SAMP board, the modem connects to a USB port on the server itself.

The modem must connect to a touch tone line, not a rotary-dial line. A telephone line connects the modem to a dedicated outside line.

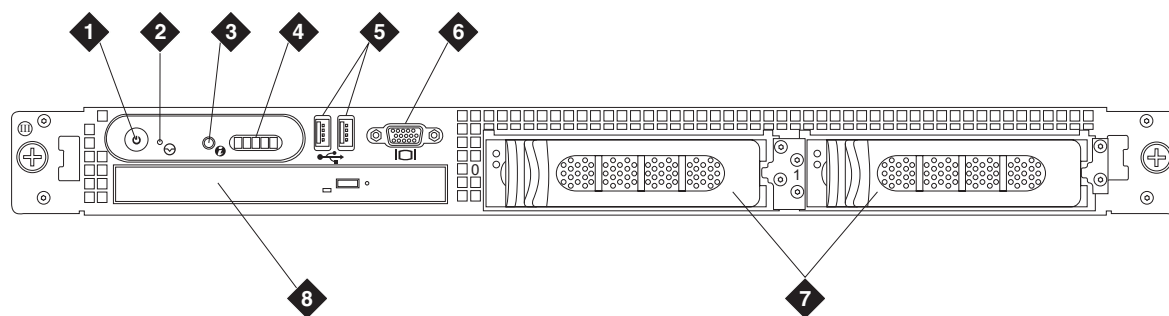
Avaya supports the MultiTech MultiModem ZBA modem for use with the S8510 server. This modem:

- provides V.92/56K download speeds and 48K upload speeds when connecting with V.92 servers.
- is Linux-compatible
- is globally approved for use in many countries worldwide
- has flash memory
- includes the USB cable.

S8510 connections

[Figure 24](#) and [Figure 25](#) show and describe the connections to the Avaya S8510 Server.

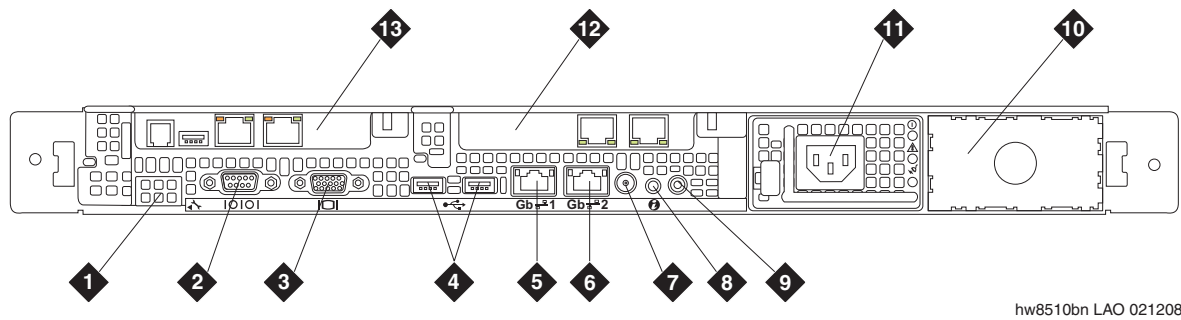
Figure 24: Avaya S8510 front panel



hw8510fn LAO 020108

Figure notes:

- | | |
|--|-------------------------------|
| 1. Power-on indicator, power button | 5. USB 2.0 connectors |
| 2. Nonmaskable Interrupt (NMI) button (disabled) | 6. Video connector (not used) |
| 3. System identification button (used to locate equipment within the rack) | 7. Hard disk drives |
| 4. LCD display (system ID, status information, and system error messages) | 8. Slimline optical drive |
-

Figure 25: Avaya S8510 (rear panel)**Figure notes:**

- | | |
|---|---|
| 1. Remote Access Controller (not populated) | 8. System Identification Button |
| 2. Serial connector | 9. System Status Indicator |
| 3. Video connector | 10. Power supply 2 (redundant and optional) |
| 4. 2-USB 2.0-compliant connections (not used) | 11. Power supply 1 |
| 5. Integrated gigabit Ethernet NIC1 (supports 10/100/1000-Mbps) | 12. Dual-NIC board |
| 6. Integrated gigabit Ethernet NIC2 (supports 10/100/1000-Mbps) | 13. SAMP board |
| 7. System Status Indicator Connector | |

Avaya S8700 Series Servers

The Avaya S8700-Series (including S8720 and S8710) servers use a standard microprocessor engine on a commercial server. The S8720 server is available in two configurations:

- Standard configuration
- Extra large configuration that provides higher capacities is available with Communication Manager R4.0 and later releases. This configuration requires the DAL2 card.

The S8700 Series Servers support two types of port network configurations, or a combination of both:

- Voice bearer over IP (IP-PNC): An all-IP configuration that carries both control and bearer information.

- Voice bearer over fiber-PNC, with direct-connect expansion interface circuit packs, Center Stage Switch (CSS), or Asynchronous Transfer Mode (ATM).

In fiber-PNC configurations, the bearer paths and control paths are separate. The control information for port networks travels over a control network. The control information terminates on the server at one end and at the IP Server Interface (IPSI) circuit pack on the other. The control network can be of one of the following:

- A dedicated control network in which an Ethernet switch is used only for the control network and, therefore, creates a private LAN
- A nondedicated control network in which control data pass through an Ethernet switch that is also connected to the customer LAN

Note:

For information on port network connectivity, see *Administering Network Connectivity on Avaya Aura® Communication Manager (555-233-504)*.

Diagrams and descriptions of access/connectivity to the currently-available S8700-Series Servers include:

- [S8720 access / connectivity](#) on page 192
- [S8730 access / connectivity](#) on page 194

Memory and software duplication

Avaya S8700-Series Servers are always configured as duplicated pairs of identical servers that can support:

- **Memory duplication** using the DAL2 memory duplication card is as an option for connections to the duplicated server. If purchased, the memory duplication option includes two DAL2 cards installed in both servers and the dual fiber cable that connects them.
- **Software duplication** eliminates the need for the DAL2 memory duplication card. If software duplication is used, the functions of the Eth0 and Eth2 interfaces are reversed with respect to the hardware duplication functions. Memory duplication messages are sent over the server duplication TCP/IP link.

Note:

Because using software duplication can reduce system performance, Avaya recommends a dedicated duplication link. If the duplication link is routed or switched, it should have a minimum bandwidth of 1 Gbps.

Fiber link between the active and standby servers

SIM and Arbiter processes

Two processes communicate over the fiber link between S87XX servers:

- **Service Interface Module (SIM)** between the server and IP Server Interface (IPSI) circuit pack in each port network that controls the hardware in the port network to make connections among endpoints (phones) and Communication Manager (call processing) resources.
SIM traffic includes caller and called-party information (phone numbers), authorization codes, and any keyed dial-pad information: credit card, Social Security, account, or any other identifying numbers. Potential harm as a result of intercepting the data on this interface includes the ability to seize trunks, redirect calls, and alter call detail recording.
- The **Arbiter** assesses the state of health of both servers, initiates shadowing actions on various state transitions, determines when a server interchange is appropriate, and manages the interchange.
The Arbiter software process determines each server's state of health and which of the server pair is better able to provide call processing. One server functions as the *active server* that provides call processing, while the duplicated *standby server* is memory-shadowed and waits, ready to take the active server role should its counterpart fail or its state of health fall below that of the standby server.
Arbiter traffic contains information about the server's state of health, and a server interchange, which alone does not disrupt service, is the greatest harm that can result from intercepting Arbiter data.

SIM and Arbiter security design overviews

SIM security includes:

- TCP transport
- All messages from the server to the IPSI and vice-versa are encrypted:
 - Messages individually wrapped inside the encryption packet
 - Encryption packet includes a cyclical redundancy check (CRC), a sequence number, and pad bytes
- Complementary code in server software and IPSI firmware

Arbiter security includes:

- UDP transport, which does not set up a connection nor negotiate a session key
- Secure backup links for both the active or standby server through a dedicated or customer network

Encryption

Both the SIM and Arbiter use Triple DES (3DES) encryption using the US Data Encryption Standard as specified by FIPS-46, FIPS-46-1, FIPS-74, and FIPS-81. Avaya utilizes the Encrypt/Decrypt/Encrypt (EDE) variation with two 56-bit shared keys, along with Cipher Block Chaining (CBC) for additional security.

Encryption initially uses a key called the Compiled-In-Key (CIK) that is compiled into both the server and IPSI code. In addition, the CIK for the SIM interface is different from the CIK for the Arbiter.

[Table 36](#) compares and describes the encryption and Security Violation Notification (SVN) attributes on the SIM and Arbiter links.

Table 36: Comparison of encryption and SVN attributes on the SIM and Arbiter links

Interface	Encryption	Encryption description	SVN	SVN description
SIM	Administrable on a per-port network basis ¹	<ul style="list-style-type: none"> Avaya complements the CIK by using Encrypted Key Exchange (EKE). Each time a socket is brought up, it uses the 128-bit Diffie-Hellman (DH) algorithm. EKE combines CIK and DH in a way that strengthens both key mechanisms. 	Yes	<ul style="list-style-type: none"> SVNs are generated when decryption fails because of a hacker's intervention, and in a short time (seconds) the SIM heartbeat handshaking times out, and the socket is torn down. The time window between the hacker's attack and the socket failing allows both the server and the IPSI to report the attack to the logmanager's debug trace log.² When the server or IPSI successfully decrypts 5,000 consecutive messages on the same socket, the logmanager's debug trace log² is updated to indicate that the security violation is over.
				1 of 2

Table 36: Comparison of encryption and SVN attributes on the SIM and Arbiter links

Interface	Encryption	Encryption description	SVN	SVN description
Arbiter	Always ³	<ul style="list-style-type: none"> • Encrypts/decrypts all messages using the same CIK on any of the redundant links (usually three). • Each message is examined before it is decrypted, and since the message is sent on each of the redundant links, there are separate decryptions of the messages on each link. 	No	
				2 of 2

1. See [Administering encryption on the SIM link](#) on page 185.

2. See [Accessing system logs through the Web](#) on page 96.

3. All traffic over the Arbiter links is encrypted (cannot be disabled).

Administering encryption on the SIM link

You can enable or disable encryption on the SIM link through the **IP Server Interface** form that is administered at the Communication Manager system access terminal (SAT).

Note:

Avaya unconditionally encrypts all traffic over the Arbiter links (cannot be disabled).

Note:

Although the System Management Interface provide for IP Server Interface (IPSI) circuit pack administration, socket encryption is enabled/disabled only on the **IP Server Interface** form through the server's SAT interface.

Socket encryption can be controlled on a per-port network basis. Depending on the redundancy strategy one or two IPSI circuit packs are required for each port network, and each IPSI (or IPSI pair) can be independently administered.

Note:

If the IPSI circuit pack is duplicated (redundant) in a port network, encryption is either on for both or off for both IPSIs.

Two suggestions for taking advantage of independent IPSI administration:

- You might want to turn encryption on for port networks that are connected through less-protected networks.
- For port networks that are connected through more protected networks, encryption can be turned off. However, see Note below regarding system performance.

To enable/disable socket encryption on the SIM link:

1. At the Communication Manager SAT type **add|change ipserver-interface n**, where **n** is a numbered IPSI interface.

Figure 26: IP Server Interface (IPSI) Administration screen

```
add ipserver-interface n

      IP SERVER INTERFACE (IPSI) ADMINISTRATION - PORT NETWORK 2

                                     IP Control? y      Socket Encryption? y
Ignore Connectivity in Server Arbitration?      Enable QoS? y
      Administer secondary ip server interface board?

Primary IPSI                                     QoS Parameters
-----
Location: 1A02                                     Call Control 802.1p: 4
      Host: ipsi-A01a                               Call Control DiffServ: 42
      DHCP ID: ipsi-A01a

Secondary IPSI
-----
Location: 1B01
      Host: ipsi-A01b
      DHCP ID: ipsi-A01b
```

2. Type **y** in the **Socket Encryption** field to enable encryption; type **n** to disable, then press **Enter**.

Note:

System performance is impacted when encryption is enabled. Generally, there is a increased network overhead of 30% using encryption, adding approximately 7 milliseconds (ms) set-up time per call. The 30% figure is based on a “standard” inbound call, which typically takes 24 ms for call set-up, compared to the approximately 31 ms call set-up time using encryption.

3. Save the changes to the form.

Physical interface

The physical interface between the active and standby servers consists of:

- DAL2 memory duplication board with 512MB of DDR SDRAM residing in the 64-bit PCI-X slot with an internal bus speed between 50-133MHz.
- Infineon V23848-M15-C56 fiber optic transceiver using a 3.3V power supply with the LC connector
- Fiber optic interface that transmits at 2.125 Gbps over a duplex cable
- Up to 10km distance separation between the servers using single-mode fiber (SMF)

The duplication connection is point-to-point and interfaces only to the same Infineon transceiver on the other server. Although the DAL2 operates at Fibre Channel Specification speeds, its packets are proprietary and *are not Fibre Channel compatible*. Further, each packet is 8b/10b encoded/decoded, a method that converts all 256 8-bit values into pre-defined 10-bit characters.

The RocketIO Multi-Gigabit Transceiver is configurable, and since the packet configuration is proprietary, Avaya uses RocketIO in User Mode to individually assign the ports ([Table 37](#)) and attributes listed in [Table 38: Rocket IO attributes \(custom\)](#) on page 189.

Table 37: RocketIO port assignments (custom)

Port	I/O	Setting/ Connection	Notes
BREFCLK	I	brefclk	Buffered clock input from 106.25MHz oscillator (not DCM output).
BREFCLK2	I	0	
CHBONDDONE	O	n/c	Channel bonding not used.
CHBONDI(3:0)	I	0	
CHBONDO(3:0)	O	n/c	
CONFIGENABLE	I	0	Reconfiguration feature not used.
CONFIGIN	I	0	
CONFIGOUT	O	n/c	
ENCHANSYNC	I	0	Channel bonding not used.
ENMCOMMAALIGN	I	1	Allows alignment with minus-comma.
ENPCOMMAALIGN	I	1	Allows alignment with plus-comma.
LOOPBACK(1:0)	I	loopback(1:0)	Controlled by hl_lpmode and hl_loopen of the control register.
POWERDOWN	I	0	
1 of 3			

Table 37: RocketIO port assignments (custom)

Port	I/O	Setting/ Connection	Notes
REFCLK	I	0	
REFCLK2	I	0	
REFCLKSEL	I	0	Selects BREFCLK instead of BREFCLK2.
RXBUFSTATUS(1:0)	O	n/c	
RXCHARISCOMMA(1:0)	O	rxchariscomma(1:0)	To receive state machine
RXCHARISK(1:0)	O	rxcharisk(1:0)	To receive state machine
RXCHECKINGCRC	O	n/c	RocketIO CRC not used
RXCLKCORCNT(3:0)	O	n/c	
RXCOMMADET	O	n/c	
RXCRCERR	O	n/c	
RXDATA(15:0)	O	rxdata(15:0)	16-bit parallel data to receive state machine and demux
RXDISPERR(1:0)	O	rxdisperr(1:0)	To disp_err bit of interrupt register
RXLOSSOFSYNC	O	rxlosssofsync(1:0)	To hl_rcv_sync bit of status register, to sync_chg bit of interrupt register
RXP, RXN	I	rxp, rxn	Differential serial input
RXNOTINTABLE(1:0)	O	rxnotintable(1:0)	To illegal_code bit of interrupt register
RXPOLARITY	I	0	
RXREALIGN	O	n/c	
RXRECCLK	O	n/c	
RXRESET	I	hl_reset	From control register
RXRUNDISP(1:0)	O	n/c	
RXUSRCLK	I	sdclk	106.25MHz output of DCM
RXUSRCLK2	I	sdclk	106.25MHz output of DCM
TXBUFERR	O	n/c	
2 of 3			

Table 37: RocketIO port assignments (custom)

Port	I/O	Setting/ Connection	Notes
TXBYPASS8B10B(1:0)	I	00	
TXCHARDISPMODE(1:0)	I	00	
TXCHARDISPVAL(1:0)	I	00	
TXCHARISK(1:0)	I	txcharisk(1:0)	From transmit state machine
TXDATA(15:0)	I	txdata(15:0)	16-bit parallel data from transmit data mux
TXFORCECRCERR	I	0	
TXINHIBIT	I	0	
TXKERR(1:0)	I	txkerr(1:0)	To tx_inv_k bit of interrupt register
TXP, TXN	O	txp, txn	Differential serial data output
TXPOLARITY	I	0	
TXRESET	I	hl_reset	From control register
TXRUNDISP(1:0)	I	n/c	
TXUSRCLK	I	sdclk	106.25MHz output of DCM
TXUSRCLK2	I	sdclk	106.25MHz output of DCM
3 of 3			

Table 38: Rocket IO attributes (custom)

Attribute	Setting	Notes
ALIGN_COMMA_MSB	TRUE	Forces the decoder to put the comma in the most significant byte of the received data
1 of 4		

Table 38: Rocket IO attributes (custom)

Attribute	Setting	Notes
CHAN_BOND_LIMIT	16	All default values; channel bonding not used.
CHAN_BOND_MODE	OFF	
CHAN_BOND_OFFSET	8	
CHAN_BOND_ONE_SHOT	FALSE	
CHAN_BOND_SEQ_(1:2)_(1:4)	000000000000	
CHAN_BOND_SEQ_2_USE	FALSE	
CHAN_BOND_SEQ_LEN	1	
CHAN_BOND_WAIT	8	
CLK_COR_INSERT_IDLE_FLAG	FALSE	Defines output RXRUNDISP to indicate the running disparity (not the clock correction flag)
CLK_COR_KEEP_IDLE	TRUE	Forces the clock correction logic to keep at least one idle sequence between packets.
CLK_COR_REPEAT_WAIT	1	Default
CLK_COR_SEQ_1_1	00110111100	K28.5 is the first byte of the idle pattern that can be repeated or omitted by the clock correction logic.
CLK_COR_SEQ_1_2	00001010000	D16.2 is the second byte of the idle pattern that can be repeated or omitted by the clock correction logic.
CLK_COR_SEQ_1_(3:4)	000000000000	Default (not used)
CLK_COR_SEQ_2_(1:4)	000000000000	Default (not used)
CLK_COR_SEQ_2_USE	FALSE	
CLK_COR_SEQ_LEN	2	
CLK_CORRECT_USE	TRUE	Enables clock correction
COMMA_10B_MASK	111111111	When all 1s causes only the values specified by MCOMMA_10B_VALUE and PCOMMA_10B_VALUE to be recognized as commas.
CRC_END_OF_PKT	K29_7	Not used
2 of 4		

Table 38: Rocket IO attributes (custom)

Attribute	Setting	Notes
CRC_FORMAT	USER_MODE	Not used
CRC_START_OF_PKT	K27_7	Not used
DEC_MCOMMA_DETECT	TRUE	Causes output RXCHARISCOMMA to indicate minus-comma detection.
DEC_PCOMMA_DETECT	TRUE	Causes output RXCHARISCOMMA to indicate plus-comma detection.
DEC_VALID_COMMA_ONLY	TRUE	Causes output RXCHARISCOMMA to reflect only valid comma characters.
MCOMMA_10B_VALUE	1100000101	The minus-comma K28.5.
MCOMMA_DETECT	TRUE	Causes output RXCOMMADET to indicate a minus-comma detected.
PCOMMA_10B_VALUE	0011111010	The plus-comma is K28.5.
PCOMMA_DETECT	TRUE	Causes output RXCOMMADET to indicate a plus-comma detected.
REF_CLK_V_SEL	1	Selects BREFCLK instead of REFCLK
RX_BUFFER_USE	TRUE	Enable receive buffer.
RX_CRC_USE	FALSE	CRC checking turned off.
RX_DATA_WIDTH	2	Selects 16-bit interface.
RX_DECODE_USE	TRUE	Enable 8b/10b in the receiver
RX_LOS_INVALID_INCR	1	Default, causes loss-of-sync state machine to reset threshold counter after receiving 1 valid character.
RX_LOS_THRESHOLD	4	Default, causes loss-of-sync state machine to indicate loss of sync after 4 invalid characters.
RX_LOSS_OF_SYNC_FSM	TRUE	Defines output RXLOFSSOFSYNC to reflect the state of the loss-of-sync state machine.
SERDES_10B	FALSE	Allows operation at full rate (above 1Gbps).
TERMINATION_IMP	50	Selects termination for 50ohm impedance at the receiver.
3 of 4		

Table 38: Rocket IO attributes (custom)

Attribute	Setting	Notes
TX_BUFFER_USE	TRUE	Enables transmit buffer.
TX_CRC_FORCE_VALUE	11010110	Not used.
TX_CRC_USE	FALSE	CRC generation turned off.
TX_DATA_WIDTH	2	Selects 16-bit interface.
TX_DIFF_CTRL	500	Selects 500mV peak-to-peak for each transmit serial output (1.0V differential).
TX_PREEMPHASIS	0	Selects least amount of pre-emphasis (10%).
4 of 4		

S8720 access / connectivity

The following figures show access to critical components of the S8720 server or to its connection ports:

- [Figure 27: S8720 Media Server \(front\)](#) on page 192
- [Figure 28: S8720 Media Server \(back\) with hardware duplication](#) on page 193
- [Figure 29: S8720 Media Server \(back\) with software duplication](#) on page 193

Figure 27: S8720 Media Server (front)

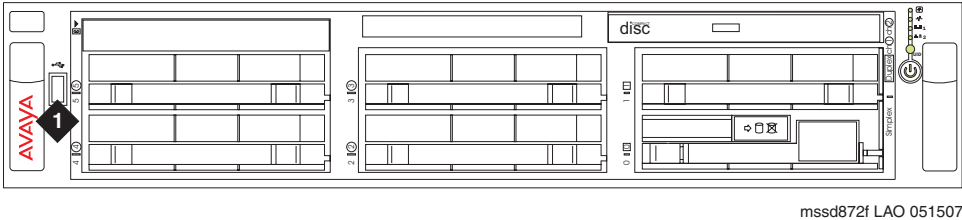
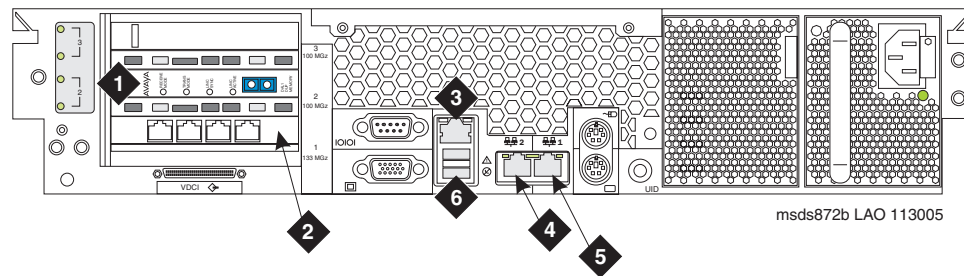
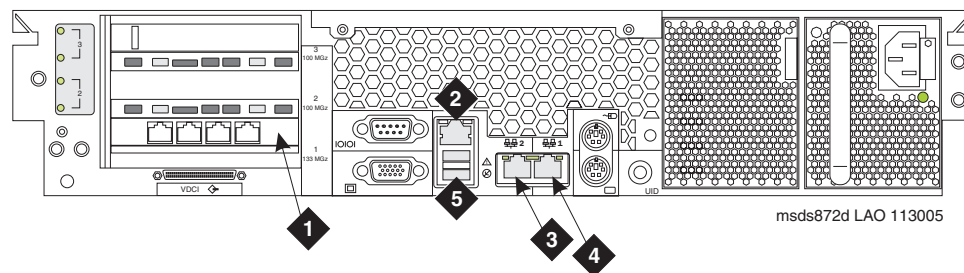


Figure notes:

Number	Description of Device
1.	CD/DVD-ROM drive

Figure 28: S8720 Media Server (back) with hardware duplication**Figure notes:**

Number	Description of Device
1.	Optional DAL1 or DAL2 Duplication board (used for memory duplication between servers when hardware duplication used)
2.	4-port NIC card, first port on left used for data duplication between servers (Eth 2)
3.	1 iLO NIC port (not used)
4.	Services port (Eth 1)
5.	Control network A (Eth 0)
6.	USB ports for modem and Compact Flash drive

Figure 29: S8720 Media Server (back) with software duplication**Figure notes:**

Number	Description of Device
1.	4-port NIC card, first port on left used for control network (Eth 2)
2.	1 iLO NIC port (not used)
3.	Services port (Eth 1)
4.	Port used for data duplication between servers (Eth 0)
5.	USB ports for modem and Compact Flash drive

The S8700-Series server connections include:

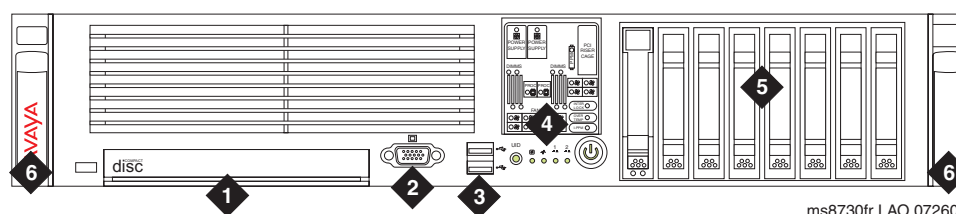
- 2 10/100/1000 Ethernet ports on the motherboard to support IPSI network control links, services access, and administration
- Three USB ports, for modem, Compact Flash drive, and other connections
- External (USB) Compact Flash
- 4-port (10/100BaseT) network interface card (quad NIC)
- A SCSI CD/DVD-ROM
- Hardware duplication is available with the optional DAL1 memory duplication card or (for the extra large configuration) the DAL2 memory duplication card with a distance limitation of 10 km between the servers.

S8730 access / connectivity

The following figures describe the access and connectivity of the S8730 server:

- [Figure 30: S8730 server \(front panel\)](#) on page 194 shows the available connections to the server's front panel.
- [Figure 31: S8730 server \(rear panel\) with hardware duplication](#) on page 195 shows the connection configuration at the rear of the server for hardware duplication.
- [Figure 32: S8730 server \(rear panel\) with software duplication](#) on page 196 shows the connection configuration at the rear of the server for software duplication.

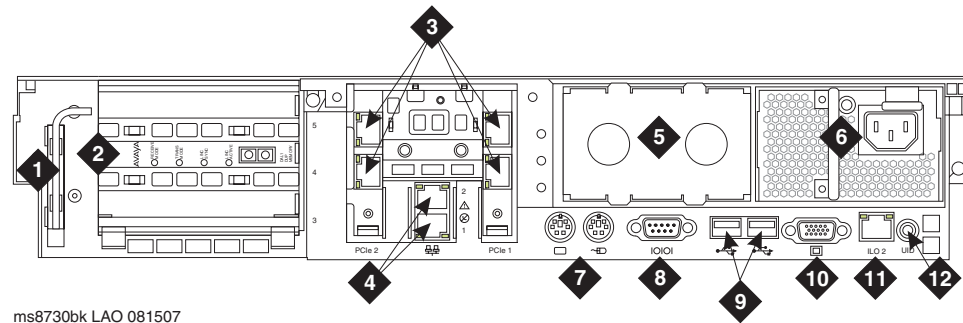
Figure 30: S8730 server (front panel)



ms8730fr LAO 072607

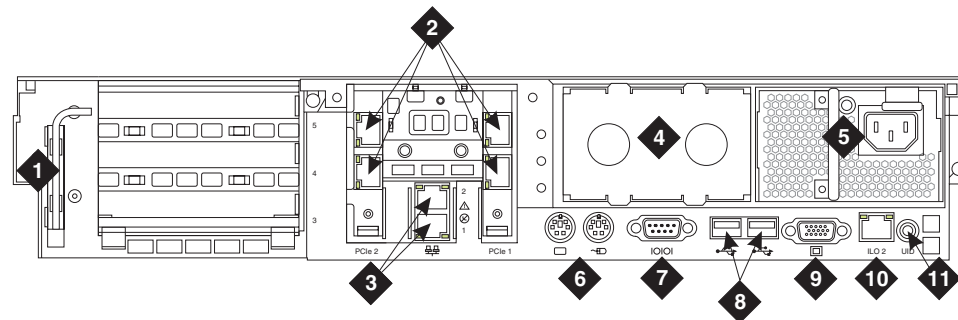
Figure notes:

- | | |
|-----------------------|-----------------------------|
| 1. CD/DVD-ROM drive | 4. Systems Insight Display |
| 2. Video connector | 5. Hard drive bays |
| 3. USB connectors (2) | 6. Quick release levers (2) |
-

Figure 31: S8730 server (rear panel) with hardware duplication**Figure notes:**

- | | |
|---|---|
| 1. Hex wrench | 7. Keyboard and mouse connectors |
| 2. Optional DAL2 Duplication board (used for memory duplication between servers when hardware duplication used) | 8. Serial connector |
| 3. Dual NICs, lower right port used for data duplication between servers (Eth 2), upper right port used for control network B (Eth 3); lower left port used for LAN (Eth 4), upper left port unused (Eth 5) | 9. USB connectors (2) for modem and Compact Flash drive |
| 4. NIC 1 and 2 connectors, top port for Services (Eth 1), bottom port for control network A (Eth 0) | 10. Video connector |
| 5. Power supply bay 2 (for optional redundant power supply) | 11. iLO 2 connector (not used) |
| 6. Power supply (bay 1 populated) | 12. Active/standby server LED |

Figure 32: S8730 server (rear panel) with software duplication



ms8730bs LAO 081507

Figure notes:

- | | |
|--|---|
| 1. Hex wrench | 7. Serial connector |
| 2. Dual NICs, lower right port used for control network A (Eth 2), upper right port used for control network B (Eth 3); lower left port used for LAN (Eth 4), upper left port unused (Eth 5) | 8. USB connectors (2) for modem and Compact Flash drive |
| 3. NIC 1 and 2 connectors, upper port for Services (Eth 1), lower port for data duplication between servers (Eth 0) | 9. Video connector |
| 4. Power supply bay 2 (for optional second hard drive) | 10. iLO 2 connector (not used) |
| 5. Power supply (bay 1 populated) | 11. Active/standby server LED |
| 6. Keyboard and mouse connectors | |

Appendix B: Network Services on Communication Manager Servers

Network service /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 C: Additional Security Resources

Documents mentioned in this security guide

This Communication Manager security guide mentions the documents that are listed in [Table 39](#).

Table 39: 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

Table 39: 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

Security documents on the Avaya support site

Security-related documents that complement this security guide are listed in [Table 40](#).

Table 40: 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
<i>Avaya Interactive Response Security</i>	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

Table 40: 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

Index

Numerical

3rd-party antivirus products	21
performance degradation	21
802.1X	
as remedy to DHCP vulnerabilities	115
authentication of Layer 2 devices	110

A

access control lists	
configuring packet filtering routers or Layer 3 switches	111
DHCP servers	115
Access Security Gateway (ASG)	18 , 79
ASG Guard.	83
credentials storage	74
description	80
password management	79
product line.	83
Address Resolution Protocol (ARP)	112
spoofing	
Domain Name System (DNS)	113
Dynamic Host Configuration Control (DHCP)	113
spoofing tool	112
Apache Web server	24
authentication	
802.1X Layer 2 devices	110
Authentication, Authorization, and Auditing (AAA) services	105
authorization	
algorithms	
HMAC-SHA 1	42
HMAC-SHA1 32	43
HMAC-SHA1 80	43
HMAC-SHA1 96	43
Avaya Installation Wizard	
Web Access Mask default settings	27
Avaya Native Configuration Manager	
Web Access Mask default settings	28
Avaya Network Region Wizard	
Web Access Mask default settings	27
Avaya Product Certificate Authority	63
components	64
Avaya Product Security Support Team (PSST).	127
Avaya Security Advisory	
interpretation	129
Avaya Security Advisory	131
organization	130

response times based on vulnerability	128 , 146
vulnerability levels	127

B

bearer network	
separation from control network	100

C

certificates	
Avaya Product Certificate Authority	63
location and permissions.	68
modifications	69
rekeyed.	69
renewal.	69
revocation	69
validated before firmware download to H.323 endpoints	66
CLI commands	
rpm-ga	17
codec	
administered within network regions	58
administering encryption	55
Communication Manager	
local host account (default).	34
logins	
craft	31
customer super-user	32
dadmin	31
inads	31
init	31
non-super-user customer	32
control network	
separation from bearer network	100
Customer Telephone Activation (CTA)	95

D

Denial of Service (DoS) attacks	
Chargen packet storm	23
Finger of death	23
Fraggle	22
H.323 / H.225v4 PROTOS	23
in DHCP clients	114
malformed or oversized packets	23
Packet relay attack	22
PING flood	22
SDP and SIP PROTOS	23

Index

Smurf/Pong	22
SNMP PROTO	23
SPANK	23
SYN flood (TCP SYN).	22
Denial of Service (DoS) protection	121
inbound trunk traffic.	121
Remote Managed Services	124
signaling groups	125
Denial of Service (DoS) remedies	
call processing overloads	121
Remote Managed Services	122
signaling group administration	124
Domain Name Server (DNS)	
remedies	116
enable DNSSEC encryption and support.	116
separate DNS servers	116
vulnerabilities.	115
Domain Name System (DNS)	
vulnerabilities.	113
Dynamic Host Configuration Control (DHCP)	
remedies	
802.1X authentication	115
limit automatic registration	114
separate servers	115
static IP addresses	114
vulnerabilities.	113 , 114

E

encryption	
algorithms	
3DES	74
AEA	43 , 57
AES	42 , 43 , 57
AES 128-bit	43 , 44
AES-128 CBC.	42 , 44
AES-128 OFB.	44
AES-128-CTR.	43
IP endpoints.	46
SRTP	45
TN circuit packs	45
application through network regions	58
ASG accounts	74
certificate authority	61
Avaya Product Certificate Authority	69 , 70
codec administration	55
digital certificates	61
enabled in license file	56 , 59
mixing encryption policies	60
private keys	24
public keys	24
Diffie-Hellman key exchange	42
public-key integration	63
Avaya Product PKI	63
signaling group administration	59

external authentication	
credentials storage	74
LDAP.	106 , 107
LDAP/RADIUS integration	107
RADIUS	106 , 107
token-based accounts	106
RSA Secure Computing SafeWord	106
RSA SecurID	106 , 108

F

file monitoring	
Tripwire.	35
file system sharing protocols (unsupported)	
Common Internet File System (CIFS).	21
Network File System (NFS)	21
Server Message Block (SMB)	21
filesync	
certificates in duplicated S8700 servers	69
transmission protocol	69
firewall	
default settings	97
IP Tables	18 , 97
IPTables	18
FTP	19

G

G250 Media Gateway	
access control lists	104 , 120
IPSec support.	102
features	102
leveraging security features for Layer 2 and Layer 3	
hardening	101
secure file transfer (HTTPS and SCP)	120
G350 Media Gateway	
access control lists	104
IPSec support.	102
features	102
leveraging security features for Layer 2 and Layer 3	
hardening	101
secure file transfer (HTTPS and SCP)	120
G650 Media Gateway.	100
Generic Routing Encapsulation (GRE)	
GRE tunnel	102

H

H.248	
encrypted link	57
secure downloads to devices.	24
H.323	
certificate validated before firmware download.	66
encrypted link	57
secure downloads to devices.	24

hard drive partitioning	18
HTTPS connection	
for IP telephones	25
to Apache Web server	24

I

IG550 Integrated Gateway	101
access control lists	104 , 120
IPSec support	102
features	102
secure file transfer (HTTPS and SCP)	120
ingress network services	17
Inter-Gateway Alternate Routing (IGAR)	100
intrusion detections system (IDS)	35
IPSec	20
compatible non-Avaya equipment	103
Layer 2 and Layer 3 hardening	102

L

Linux operating system	
hardening	18
logging/monitoring	
privilege escalation	33
superuser	33

M

Maintenance Web Pages	
access to Communication Manager	25
Add Trap Destination page	89
Agent Status page	86
default profiles	26
Firewall page	97
IPTables firewall	18
Profile 18 permissions	27
Profile 19 permissions	27
SNMP Agents page	86
SNMP Traps page	88
Syslog Server page	91
System Logs page	95
Web Access Mask default settings	27
modem	
SAMP	179
Motorola CN620 Mobile Office Device	102

N

Name Service Caching Daemon (NSCD)	
LDAP servers	107
Name Service Switch (NSS)	
LDAP servers	107
National Institute of Standards and Technology (NIST)	

remedies	
availability and denial of service	120
account lockout vulnerability	121
forced system restart	120
confidentiality and privacy	116
ARP cache poisoning/floods	117
default password	117
IP address mapping	118
IP phone subnet mask	118
packet sniffer/protocol analyzer	117
Web server interfaces	118
integrity issues	119
DHCP server insertion attack	119
TFTP server insertion attack	120
security risks in VoIP systems	116
network regions	
administering codecs	58
inter-network region connections	60
network separation	100
802.1X authentication	111
restricting VLAN traffic	111
standard network services	111
stateful filtering	111
VLAN design	110
non-secure protocols	
FTP	19
TELNET	19

O

Open Systems Interconnect (OSI)	101
operating system	
Linux	
hardening	17 , 18
Red Hat Package Management (RPM)	17

P

passwords	
where stored	74
Personal Station Access (PSA)	95
privilege escalation	
logging location	33
Product Security Support Team (PSST)	127
Property Management System (PMS)	94

R

Red Hat Package Management (RPM)	
command to generate list	17
modules removed	17
regulatory compliance	
FISMA	156
regulatory compliance (non-USA)	162

Index

Basel II.	162
regulatory compliance (USA)	
CALEA.	155
E/911	160
IP telephony.	161
traditional telephony	161
Gramm-Leach-Bliley Act	152
HIPAA	153
ISO 17799	157
Sarbanes-Oxley Act.	150
Remote Feature Activation (RFA).	68
role based access control (RBAC)	
privilege escalation	33
role evaluation	75
SAT and Web profile administration	75

S

S8300 Server	
access/connectivity	168
hardware description	167
S8400 Server	
access/connectivity	169
cable adapter.	174
hardware description	168
SSD vs. HDD.	170
TN8400AP Media Server circuit pack	168
TN8412AP S8400 IP Interface (SIPI) circuit pack	168 , 172
S8500 Server	175
128-MB Compact Flash	178
access/connectivity	175
hardware description	177
SAMP	177
SAMP remote maintenance	177
S8700-Series Servers	181
access/connectivity	192
hardware description	194
SAMP	
modem.	179
Secure Computing SafeWord	
token servers.	108
secure protocols	
DES	89
MD5	89
Secure Copy (SCP).	19 , 115 , 164
Secure Shell (SSH).	17 , 19
SNMPv3	19 , 85 , 88 , 89
Secure Socket Layer (SSL).	17
security notifications	
SNMP and syslog.	84 , 101
syslog	90
administration	91
logging levels	92
priority and facility	85

where logged	132
security updates	
contents	148
field load or software update	148 , 164
operating system	147
vulnerability levels and remediation intervals	146
security violations.	136
Server Availability Management Processor (SAMP).	177
Simple Authentication and Security Layer (SASL).	74 , 80
SIP Enablement Services (SES).	44
SIP-TLS connections	
PKI integration (digital signatures)	24
SNMP	
agent access SAT profile	32
community strings	20
security-related events sent to Remote Managed Services.	122
SNMPv3	19 , 85 , 88 , 89
SNMPv3/v2c	
community name	19
software update	
3rd-party	131
PKI authentication	25
SRTTP	
media encryption	43
superuser	
see user account/profile	33
syslog	
log interpretation	133
Communication Manager command history log	139
header	133
platform command history log	135
SNMP entries	134
Web command history log	141
restricting Web access to	132
stored locally or exported to external server	90
System Access Terminal (SAT)	
access to Communication Manager.	26
default profiles	31
feature-related system parameters form	121
logging levels form	93
profile default settings	32
security-related system parameters.	123
system intrusion	
Tripwire.	35

T

TELNET	19
Terminal Translation Initialization (TTI).	95
TN2312BP (IPSI) circuit pack	100
toll fraud	83
Transport Layer Security (TLS)	20 , 63
Tripwire	35 , 101
policy file	35

U

user account/profile	
credentials storage	74
default Maintenance Web Page accounts	26
password aging	72
password complexity	71
privilege escalation	18 , 33
removing old accounts	132
role based access control (RBAC)	26 , 27
service accounts	
password aging	80
superuser	
logging location	33
permissions and restrictions	33
System Access Terminal (SAT) default accounts	31

V

viruses	
effects on VOIP system	20

W

worms	
effects on VOIP system	20

X

XINETD	18
------------------	--------------------

