Avaya Aura® Communication Manager Security Design

Release 6.3
03-601973
Issue 6
May 2013

Notice

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

Warranty

Avaya provides a limited warranty on its hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants you a license within the scope of the license types described below, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

- Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.
- Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than an Instance of the same database.

- CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.
- Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products". For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

Each Product has its own ordering code. Note that each instance of a Product must be separately licensed and ordered. "Instance" means one unique copy of the Software. For example, if the end user customer or Avaya channel partner would like to install two instances of the same type of Products, then two Products of that type must be ordered.

How to Get Help

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

- Within the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the appropriate link for the type of support that you need.
- Outside the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the International Services link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

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

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

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

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

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

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

Responsibility for Your Company's Telecommunications Security

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

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

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

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

TCP/IP Facilities

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

Product Safety Standards

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

- IEC 60950-1 latest edition, including all relevant national deviations as listed in the IECEE Bulletin—Product Category OFF: IT and Office Equipment.
- CAN/CSA-C22.2 No. 60950-1 / UL 60950-1 latest edition.

This product may contain Class 1 laser devices.

- Class 1 Laser Product
- Luokan 1 Laserlaite
- Klass 1 Laser Apparat

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards, as applicable:

- CISPR 22, including all national standards based on CISPR 22.
- CISPR 24, including all national standards based on CISPR 24.
- IEC 61000-3-2 and IEC 61000-3-3.

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

Federal Communications Commission Part 15 Statement:

For a Class A digital device or peripheral:

Note:

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

For a Class B digital device or peripheral:

Note:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Equipment With Direct Inward Dialing ("DID"):

Allowing this equipment to be operated in such a manner as to not provide proper answer supervision is a violation of Part 68 of the FCC's rules.

Proper Answer Supervision is when:

1. This equipment returns answer supervision to the public switched telephone network (PSTN) when DID calls are:
   - answered by the called station,
   - answered by the attendant,
   - routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user
   - routed to a dial prompt
2. This equipment returns answer supervision signals on all (DID) calls forwarded back to the PSTN.

Permissible exceptions are:

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

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

Automatic Dialers:

When programming emergency numbers and (or) making test calls to emergency numbers:

- Remain on the line and briefly explain to the dispatcher the reason for the call.
- Perform such activities in the off-peak hours, such as early morning or late evenings.

Toll Restriction and least Cost Routing Equipment:

The software contained in this equipment to allow user access to the network must be upgraded to recognize newly established network area codes and exchange codes as they are placed into service.

Failure to upgrade the premises systems or peripheral equipment to recognize the new codes as they are established will restrict the customer and the customer's employees from gaining access to the network and to these codes.

For equipment approved prior to July 23, 2001:

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

For equipment approved after July 23, 2001:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council on Terminal Attachments (ACTA). On the rear of this equipment is a label that contains, among other information, a product identifier in the format

US:AAAEQ##TXXX. If requested, this number must be provided to the telephone company.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0.

L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas cinq.

To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXX. The digits represented by ## are the REN without a decimal point (for example, 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Means of Connection:

Connection of this equipment to the telephone network is shown in the following table:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2.T	AS.2	RJ2GX, RJ21X, RJ11C
CO trunk	02GS2	0.3A	RJ21X, RJ11C
	02LS2	0.3A	RJ21X, RJ11C
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9.BN	6.0F	RJ48C, RJ48M
	04DU9.1KN	6.0F	RJ48C, RJ48M
	04DU9.1SN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9.DN	6.0Y	RJ48C

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

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

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

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

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Installation and Repairs

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

Repairs to certified equipment should be coordinated by a representative designated by the supplier. It is recommended that repairs be performed by Avaya certified technicians.

FCC Part 68 Supplier's Declarations of Conformity

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

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

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

Canadian Conformity Information

This Class A (or B) digital apparatus complies with Canadian ICES-003.

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

This product meets the applicable Industry Canada technical specifications/Le présent materiel est conforme aux specifications techniques applicables d'Industrie Canada.

European Union Declarations of Conformity

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (Conformité Europeénne) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (2004/108/EC) and Low Voltage Directive (2006/95/EC).

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

European Union Battery Directive

Avaya Inc. supports European Union Battery Directive 2006/66/EC. Certain Avaya Inc. products contain lithium batteries. These batteries are not customer or field replaceable parts. Do not disassemble. Batteries may pose a hazard if mishandled.

Japan

The power cord set included in the shipment or associated with the product is meant to be used with the said product only. Do not use the cord set for any other purpose. Any non-recommended usage could lead to hazardous incidents like fire disaster, electric shock, and faulty operation.

本製品に同梱または付属している電源コードセットは、本製品専用です。本製品以外の製品ならびに他の用途で使用しないでください。火災、感電、故障の原因となります。

If this is a Class A device:

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

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

If this is a Class B device:

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラス Ｂ 情報技術装置です。この装置は，家庭環境で使用することを目的としていますが，この装置がラジオやテレビジョン受信機に近接して使用されると，受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

This book is designed to provide a certain level of security-related information.

Intended audience

This document is intended for anyone who wants to gain a high-level understanding of Communication Manager security, tackling vulnerabilities, and making the communications system of an organization safe and secure.

Document changes since last issue

The following changes were made in this document since the last issue:

- Updated the output of the **`change ip-network-region`** command in Administer encryption for IP CODEC sets through SAT on page 51.

Related resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Design		

Title	Description	Audience
Avaya Aura® Communication Manager Security Design, *03-601973*	Describes the security-related information.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
Implementation		
Implementing Avaya Aura® Communication Manager, 03-603558	Describes the implementation instructions for Communication Manager.	Implementation Engineers, Support Personnel
Avaya Aura® Communication Manager Feature Description and Implementation, 555-245-205	Describes the features of Communication Manager and instructions to implement the features	Implementation Engineers, Support Personnel
Maintenance and Troubleshooting		
Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers, 03-300431	Describes the commands for Communication Manager.	Implementation Engineers, Support Personnel
Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers, 03-300432	Describes maintenance procedures for Communication Manager	Implementation Engineers, Support Personnel
Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers, 03-300430	Describes maintenance alarms for Communication Manager	Implementation Engineers, Support Personnel
Administration		
Administering Avaya Aura® Communication Manager, 03-300509	Describes the procedures and screens for administering Communication Manager.	Implementation Engineers, Support Personnel
Administering Avaya Aura® Communication Manager, 03-300509	Describes steps to administer Communication Manager	Implementation Engineers, Support Personnel
Administering Network Connectivity on Avaya Aura® Communication Manager, 555-233-504	Describes steps to administer network connectivity in Communication Manager	Implementation Engineers, Support Personnel

Title	Description	Audience
Understanding		
Avaya Aura® Communication Manager Feature Description and Implementation, 555-245-205	Describes the features that you can administer using Communication Manager.	Implementation Engineers, Support Personnel
Avaya Toll Fraud and Security Handbook, 555-025-600	Describes steps to prevent toll fraud in Communication Manager	Implementation Engineers, Support Personnel
Avaya Aura® Communication Manager Hardware Description and Reference, 555-245-207	Describes various hardware devices used for Communication Manager	Implementation Engineers, Support Personnel
SNMP Reference Guide for Avaya Communication Manager, 03-602013	Serves as a a reference guide for the simple network management protocol	Implementation Engineers, Support Personnel

Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to http://support.avaya.com, select the product name, and select the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Note:

Videos are not available for all products.

Training

The following courses are available on https://www.avaya-learning.com. To search for the course, in the **Search** field, enter the course code and click **Go**.

Course code	Course title
1A00234E	Avaya Aura® Fundamental Technology
4U00030E	Avaya Aura® Communication Manager and CM Messaging Implementation
ATC00838VEN	Avaya Media Servers and Implementation Workshop Labs
AVA00383WEN	Avaya Aura® Communication Manager Overview
AVA00279WEN	Communication Manager - Configuring Basic Features
ATI01672VEN, AVA00832WEN, AVA00832VEN	Avaya Aura® Communication Manager Fundamentals
ATI02348IEN, ATI02348VEN	Avaya Aura® Communication Manager Implementation
AVA00836H00	Communication Manager Basic Administration
AVA00835WEN	Avaya Communication Manager Trunk and Routing Administration
5U00040I	Avaya Aura® Communication Manager Maintenance and Troubleshooting
5U0041I	Avaya Aura® Communication Manager Administration
AVA00833WEN	Avaya Communication Manager - Call Permissions
AVA00834WEN	Avaya Communication Manager - System Features and Administration
4U00121W	Avaya Aura® Communication Manager Technical Delta R6.2
Docu00158	Whats New in Avaya Aura® Release 6.2 Feature Pack 2
4U00115V	Avaya Aura® Communication Manager Implementation Upgrade (R5.X to 6.X)
4U00115V	Avaya Aura® Communication Manager Implementation Upgrade (R5.X to 6.X)

Avaya information classifications

Avaya divides security-related information into the following information classifications.

Since this book is generally available, the information herein is considered public. 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.

Table 1: Avaya information classifications

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

Communication Manager security philosophy overview

This document describes the security-related considerations, features, and services for Communication Manager and the servers that run Communication Manager. The communication system of an organization must 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 and the unauthorized use of communications resources. However, the IP Telephony capabilities of Communication Manager, which converge telephony services with services on the enterprise data network, have the additional need for protection that were previously specific only to data networking. Telephony services must be protected from security threats such as:

- Denial of Service (DoS) attacks
- Theft of data
- Theft of service
- Worms
- Viruses

Responsibility for Communication Manager security

Avaya is responsible for designing and testing all Avaya products for security. When Avaya sells a product as a hardware/software package, the design and testing process of the Avaya product also includes the testing of the operating system. Avaya modifies the operating system for increased system performance and to protect against security vulnerabilities that can heavily impact an enterprise.

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

Responsibility for security updates

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

Avaya notifies customers of the availability of security updates through Security Advisories. Customers can subscribe for these Security Advisories by e-mail. For further information, see Description of Avaya Security Advisory on page 125 and Timeframe of Avaya Security Advisories on page 125.

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

Product-specific security guides of Avaya

This document describes security-related issues and security features of Communication Manager, the Communication Manager Servers, and, when applicable, security features of telephones and 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 and 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

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Warranty

Avaya provides a 90-day limited warranty on Communication Manager. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Communication Manager in the warranty period is available on the Avaya Support website at http://

support.avaya.com/ under **Help & Policies** > **Policies & Legal** > **Warranty & Product Lifecycle**. See also **Help & Policies** > **Policies & Legal** > **License Terms**.

Chapter 2: Communication Manager Security Overview

Secure by design

Secure by design encompasses a secure deployment strategy that separates servers providing communication services from the enterprise production network. Gateways protect and isolate Communication Manager from viruses, worms, DoS, and other malicious attacks.

In the figure on page 20, the architecture design is related to the trusted communication framework, infrastructure, and security layer. With this architecture, enterprises can design dedicated security zones for:

- Administration
- Gateway control network
- Enterprise network
- Adjuncts

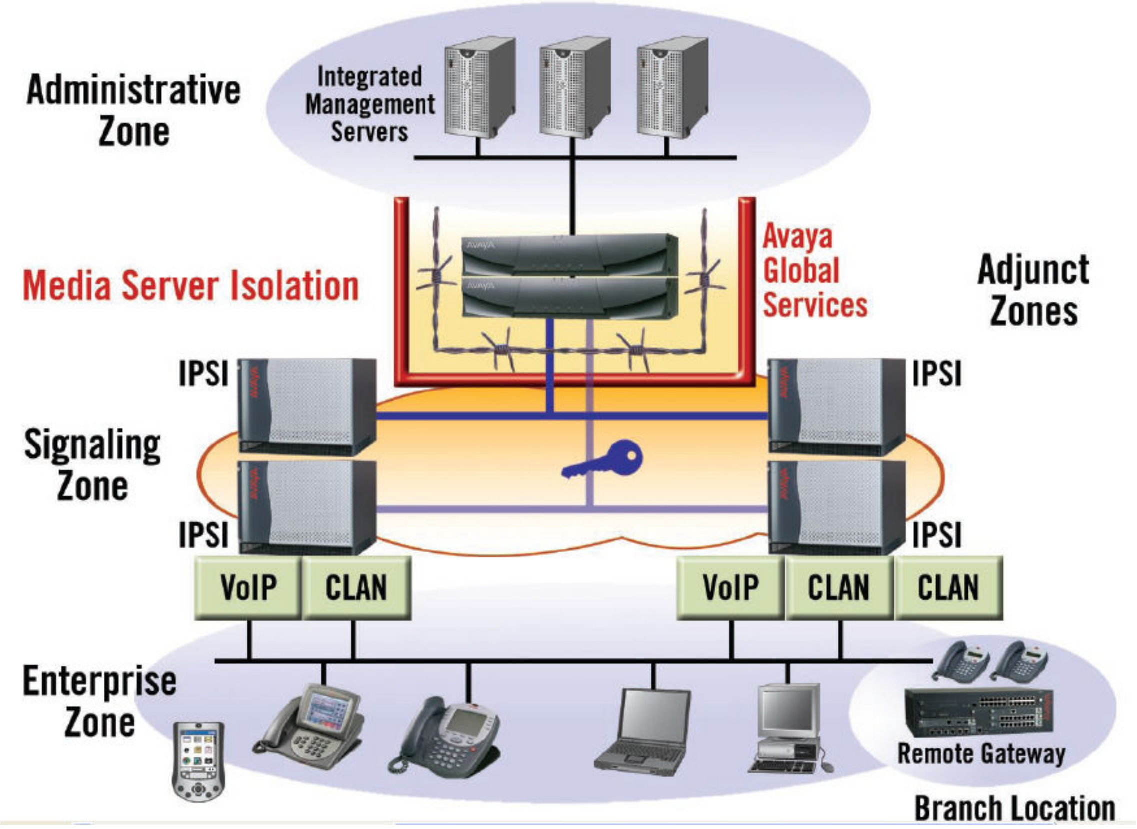


Figure 1: Avaya secure by design architecture

Avaya isolates assets so that each secure zone is inaccessible from the enterprise or branch office zones. The zones are similar to dedicated networks for particular functions or services. The zones accommodate zone-specific data without the need to gain access from or to other zones. This architecture provides protection against attacks from within the enterprise and branch office zone. The the figure on page 20 shows that you can gain access into the red Server zone through the range of endpoints and branch office gateways used for signaling traffic.

Gateways with dedicated gatekeeper front-end interfaces, such as CLANs, inspect the data traffic, and protect the Server zone from flooding attacks and malformed IP packets. The dedicated front-end interface also prevents a hacker to gain unauthorized administrative access of the Server through the Gateways.

This secure by design architecture and framework also flexibly enhances the virtual enterprise and integrates branch offices into the main corporate network. The security zone from the branch office can stop at the central Gateway interfaces protecting Communication Manager.

Secure by default

Secure by default, the second security layer of Avaya, incorporates a hardened Linux operating system with inherent security features for Avaya Servers and Communication Manager. The hardened Linux operating system provides only the functions necessary to support the core applications. The hardened Linux operating system supports the core applications that are important for:

- securing mission-critical call processing applications
- protecting the customer from toll fraud and other malicious attacks

Avaya modifies and hardens the standard Linux kernel to provide for secure, real-time telephony processing.

The Linux operating system that Avaya has hardened limits the number of access ports, services, and executable files. The limitations of the Avaya-modified Linux operating system help protect the system from typical modes of attacks. The elimination of some functions from Linux reduces the number of mandatory security patches needed and the risk of the narrow vulnerability-to-exploit time window.

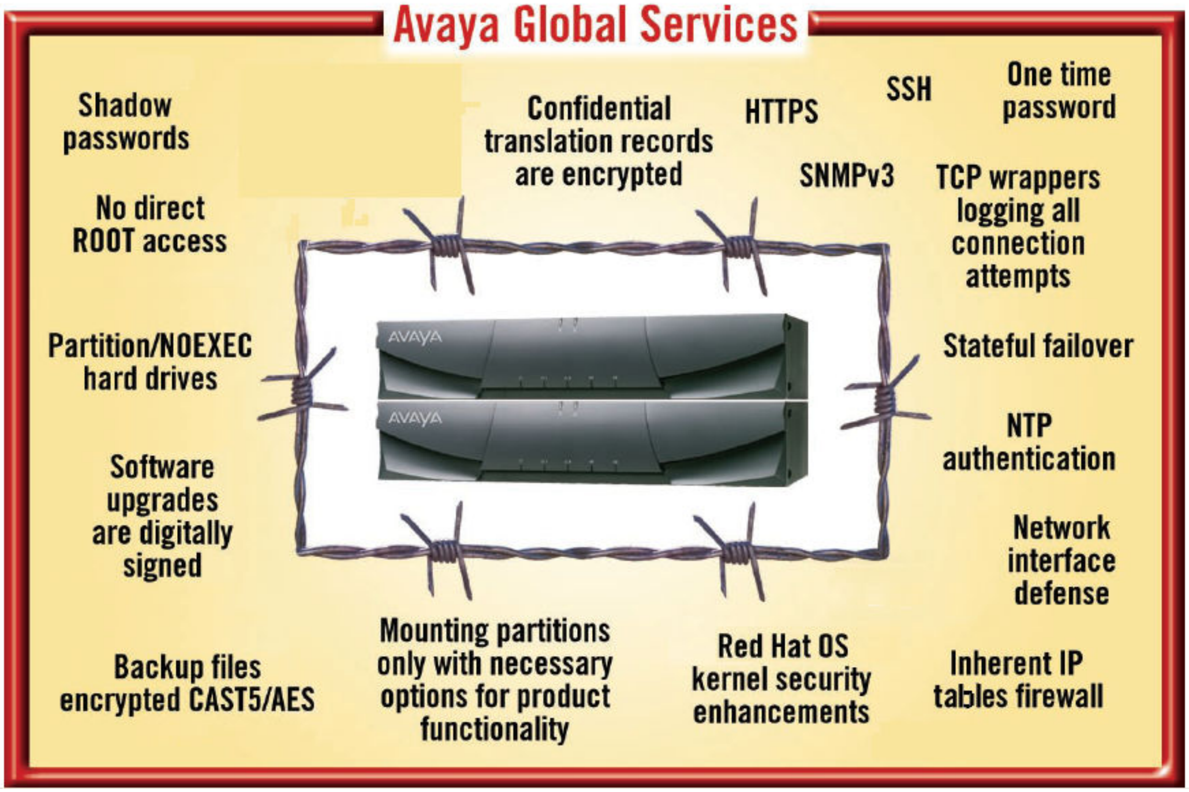

Avaya Global Services
Shadow passwords
Confidential translation records are encrypted
HTTPS
SSH
One time password
SNMPv3
No direct ROOT access
TCP wrappers logging all connection attempts
AVAYA
AVAYA
Partition/NOEXEC hard drives
Stateful failover
NTP authentication
Software upgrades are digitally signed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

Figure 2: Avaya Global Services security

Communication Manager provides a range of in-built functionalities to address the threats posed by malicious software. The functionalities eliminate the need for a co resident antivirus software. The co resident antivirus software can interfere with call processing functions and can require continuous administrative attention to ensure that the antivirus databases are up-to-date.

Secure communications

Secure communications, the third layer of the hardening strategy of Avaya, uses numerous features and protocols to protect access to and the transmissions from Avaya communications systems. Communication Managerand the gateways of Communication Manager use encryption to ensure privacy for the voice stream. With encryption, integrated signaling security protects and authenticates messages to all connected gateways and IP telephones and eliminates tampering with confidential call information. These features protect sensitive information of:

- Caller
- Called party numbers
- User authorization
- Barrier codes
- Credit card numbers
- Other personal information that a user dials during calls to banks or automated retailers.

You can encrypt critical adjunct connections, for example, the CTI link, which you can separate in a dedicated security zone.

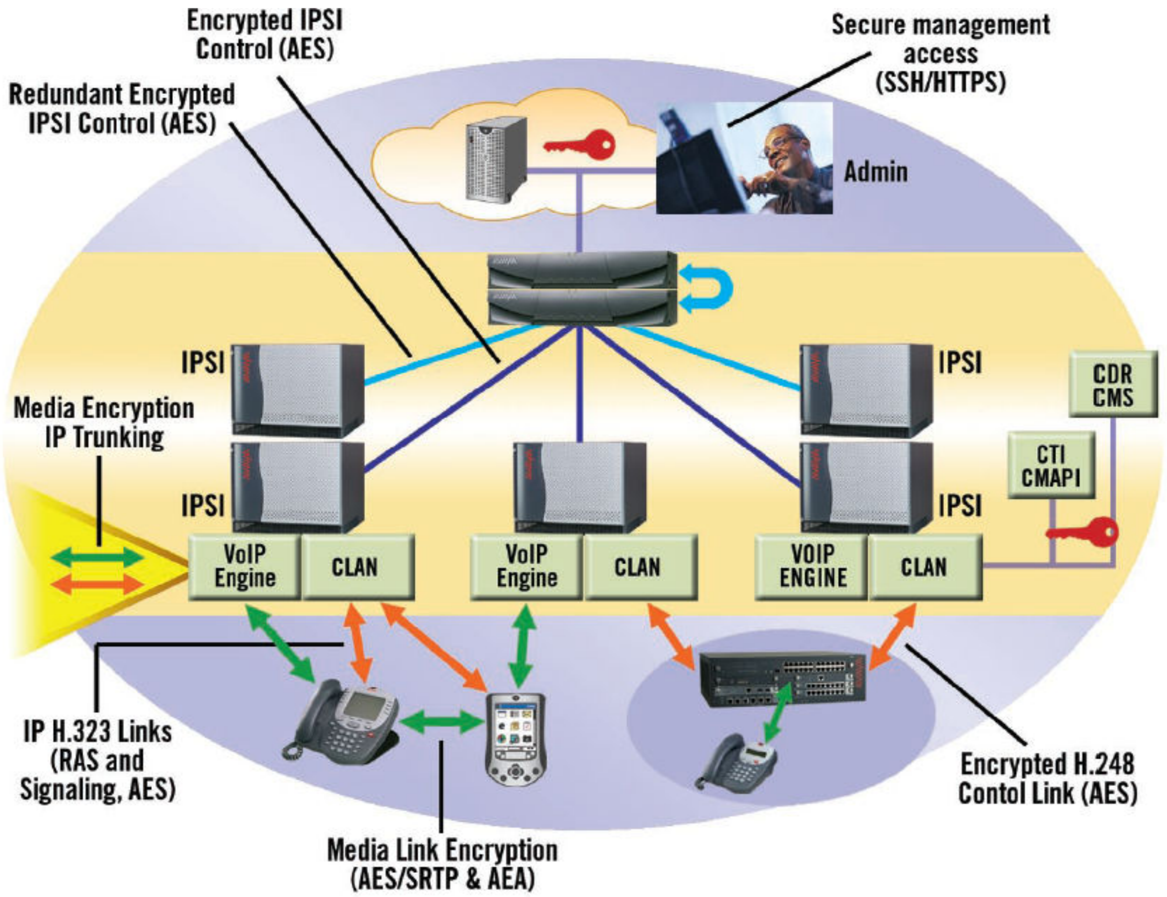

Encrypted IPSI Control (AES)
Secure management access (SSH/HTTPS)
Redundant Encrypted IPSI Control (AES)
Admin
IPSI
IPSI
Media Encryption IP Trunking
IPSI
IPSI
CDR CMS
CTI CMAPI
VoIP Engine
CLAN
VoIP Engine
CLAN
VOIP ENGINE
CLAN
IP H.323 Links (RAS and Signaling, AES)
Encrypted H.248 Contol Link (AES)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

Figure 3: Avaya secure communications architecture

Avaya IP endpoints can also authenticate to the network infrastructure by supporting supplicant 802.1X. Network infrastructure devices, gateways, or data switches function as authenticators and forwards this authentication request to a customer authentication service.

Operating system hardening

Linux as the chosen operating system for Communication Manager

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

The following are some of the benefits of the open source foundation:

- Security experts worldwide review the source code looking for defects and vulnerabilities.
- Before incorporating any changes into Avaya products, the developers and testers at Avaya supervise and review the enhancements and improvements that the Linux community creates.
- Linux-based Avaya servers and gateways protect against any Denial of Service (DoS) attacks such as SYN floods, ping floods, malformed packets, oversized packets, and sequence number spoofing.

> **Note:**
>
> Because of operating system hardening, Communication Manager does not respond to the following:
>
> - ICMP timestamp
> - TCP timestamp
> - Address-mask queries
> - Broadcast ping

Approach of Avaya to improve Linux

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

RPMs removed

The Linux general distribution includes Red Hat Package Management (RPM) modules that install, remove, verify, query, and update software packages. For IP telephony applications, Avaya requires only 30% of the nearly 800 distributed RPMs. Therefore, Avaya has removed all unused RPMs from the Linux general distribution. For example, tcpdump and wireshark (ethereal) packet capturing tools are two of the RPMs that Avaya has removed. Removing unused RPMs makes the software file images smaller and more manageable. The operating system also becomes more secure as hackers cannot change RPMs that are not present.

Viewing RPMs

About this task

Use this procedure to view the RPMs that Avaya uses.

Procedure

On the SAT screen, type **`rpm -qa`**.

Unnecessary IP ports closed

Many Linux modules such as SSH, Apache, or SSL/TLS (HTTPS) are applications that open Ingress network services. Avaya uses the Ingress network services only for telephony applications, minimizing the risk for network-based attacks. By default, Avaya disables less secure network services such as Telnet and FTP, although customers can enable these network services when required. For more information, refer to section Benefits of using SSH/SCP on page 26.

Firewall protection

The Linux-based products of Avaya use the IPTables firewall that protects the system against various network-based attacks. The firewall also protects against Ingress services that the XINETD process activates. The XINETD process listens for incoming connection requests on specific ports and runs the services related to the ports.

Using the Communication Manager System Management Interface that manages the host-based IPTables firewall, customers can control open and closed ports to accommodate for network security requirements.

Drive partitioning

File and folder permissions minimize access and act as a preventive measure against malware and tampering. For more information, refer to section Protection from viruses and worms on page 27. Some of the benefits of drive partitioning are:

- You can store the executable files in separate hard drive partitions.
- You can store the data in separate partitions. The data files do not have the execute permissions (the NOEXEC flag).

Linux operating system kernel hardening

Avaya modifies the Red Hat Linux operation system to maximize security and to meet the demands of real-time telephony processing. The real-time telephone processing demands include handling finer-grained timing increments. Most of the Linux community kernel advisories have no impact on Avaya as the operating system kernel modifications makes Avaya inherently immune to security-related attacks.

Privilege escalation and root logins

The Linux-based products of Avaya adopt the “privilege escalation” concept. The concept of privilege escalation requires lower-privileged accounts to log in at a normal level before escalating privileges to perform more restrictive tasks, such as software upgrades. Each privilege escalation requires a password or ASG response and creates an entry in the log file for monitoring and tracking.

Tip:

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

Access Security Gateway

Access Security Gateway (ASG) is a challenge-response authentication system that replaces passwords for administrative or technical support accounts. When you try to log in to a server, the system displays a randomly generated number instead of prompting for a password. You can use the number to perform a calculation to determine the correct response and gain access to the server only after entering the correct response.

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

Benefits of using SSH/SCP

Protocols that carry unencrypted sensitive data, such as logins and passwords, can cause a serious security risk to a client using VoIP. Protocols that carry encrypted data, such as SSH and SFTP, protect critical data from hackers. Partly because of new legislation and stricter auditing requirements, Avaya has implemented more secure protocols to enforce a secure connection design architecture.

By default, Avaya disables the following network services, which are not secure:

- TELNET (TELetype NETwork): Telnet does not encrypt login IDs, passwords, or PIN information sent between two computers.
- FTP (File Transfer Protocol): FTP sends information in unencrypted text, which eavesdroppers can intercept and read. Also, FTP has no integrity check, therefore if the eavesdroppers interrupt a file transfer, the recipient cannot determine if the file transfer completed successfully.

Note:

If a customer chooses to use FTP or TELNET or both, the customer can enable the functionality in certain products, but the fuctionality remains disabled by default.

Using the following protocols, Avaya products protect the authentication credentials and file transfers, when sent across the network:

- Secure Shell (SSH)
- Secure Copy (SCP) or Secure File Transfer Protocol (SFTP)
- SNMP with the following specifications:
    - SNMPv3 is the preferred version because of a built-in security mechanism.
    - SNMPv1 or v2c, while supported, provides only a limited security capability based on community names.
    - The community name for SNMPv1 and SNMPv2c is unprotected for read-only MIBs:
    - The community name for SNMPv1 and SNMPv2c is protected when accessing writable MIBs.

  SNMP security codes, for example, community strings, are customer-administrable.
- Other protocols protected using a Transport Layer Security (TLS) or Internet Protocol Security (IPSEC) connection

Avaya Services

Non-secure data networks such as the Internet and SNMP notifications protect the data transmission to and from Avaya Services for customer equipment. For more information about Avaya services, refer*Avaya Enterprise Services Platform Security Overview* to.

Protection from viruses and worms

Most viruses and worms, sometimes called malware, can have the following effects

- Disrupting or delaying normal functionality
- Changing configurations by rewriting code
- Exposing sensitive information

Although similar in functionality, viruses and worms differ in behavior. Opening an infected email, visiting infected web sites, or sharing file systems commonly deliver viruses or worms. A worm does not need a host or any user action. For more information, refer tothe table on page 28.

Table 2: Security impacts from viruses and worms

Security implementation	Security impact
Natural immunity	Linux-based servers of Avaya *do not* support: • Incoming or forwarding email • User Web browsing • Network File System (NFS) or Common Internet File System (CIFS), formerly Server Message Block (SMB) file system sharing protocols
File permissions	The superusers (root) with write permissions can install programs, resulting in few virus outbreaks within the Linux operating system.
Performance degradation	Avaya has tested third-party, host-based antivirus products on Linux-based servers of Avaya and uncovered significant performance degradation. Customers must not install such antivirus products on the Linux-based servers of Avaya.
Antivirus products	Customers have successfully used third-party antivirus packages on selected Avaya products. Although, virus and worm attacks are minimal because of the hardening of the operating system. For customers who prefer to install antivirus software, customers must perform a scan only when the server is under minimal or no load so that impact to the user is minimum.

Protection from Denial of Service (DoS) attacks

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

Communication Manager servers survive the DoS attacks listed in the table on page 28 without loss of function, without restarting, and without reloading. Communication Manager servers automatically recover to full service after the DoS attack.

Table 3: Avaya design against types of DoS attacks

Attack type	Description
SYN flood (TCP SYN)	Fake TCP SYN packets from random IP addresses at a rapid rate fill the connection queue and deny TCP services to legitimate users.
Land	The Land attack combines IP spoofing with opening a TCP connection. The Land attack sends a request to open a TCP connection, when the SYN flag in the header is on, but changes the IP address of the source. The Land attack changes the IP address

Attack type	Description
	of the source so that the source IP address is the same as the destination IP address. When the destination receives the packet, the destination sets an SYN, ACK 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 source, so the source keeps sending the ACK packet back expecting an updated sequence number. This puts the source into an ACK loop.
Smurf / Pong	Large numbers of ICMP echo or ping messages sent with the forged address of the intended victim. The Layer 2 devices issue an echo reply or 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 that results in an infinite loop of echo and reply messages.
Packet replay attack	Packet replay refers to the recording and re-transmission of message packets in the network. Packet replay is a significant threat for programs that require authentication sequences as an intruder can replay legitimate authentication sequence messages to gain access to a system. An attacker can replay the same packet at different rates, and the system attempts processing duplicate packets causing the following: • Total resource depletion • Termination of existing connections • Chaos in the internal buffers of the existing running applications • System abnormally shuts down in some cases
PING flood	As many ping utilities support ICMP echo requests, a person can inadvertently send a huge number of PING requests that can overload network links causing resource depletion.
Finger of death	The attacker continuously sends finger requests to a specific computer without disconnecting. Failure to terminate the connection can quickly overload the process tables of the server. The finger listen port number is 79 (see RFC 742).
Chargen packet storm	The attacker can spoof the chargen service port, port number 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	Protocol handlers stop functioning when malformed packets are sent in odd formations or the malformed packets are sent as part of the protocol. Oversized packet attacks place data in an order that does not adhere to specification or the attacks can create packets that are larger than the maximum permitted size.

Attack type	Description
SPANK	The target responds to TCP packets sent from a multicast address causing a DoS flood on the target 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. For information, log on to 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 anomalous values that cause error conditions. For more information, log on to http://www.ee.oulu.fi
SDP and SIP PROTOS	This attack uses 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. For more information, see http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/index.html.

For more information on preventing DoS attacks, see section Recommendations for preventing DoS attacks on page 119.

Digital certificates

Security problems addressed by digital certificates

Digital certificates provide:

- Secure authentication: The sender and the receiver validate each other's public key to validate each other.
- Data integrity: The data exchanged between the sender and receiver is digitally signed. The receiver can validate the digital certificate and can determine whether the data is modified or not.

Communication Manager uses digital certificates 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.

Signed firmware assures data integrity

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

- Digital certificates indicate that a message comes from the purported sender by determining that only the sender knows the private key that corresponds to the public key. Without the private key, the system cannot create a valid digital certificate.
- Timestamp documents. A trusted party signs the document and the timestamp of the document with the private key, assuring that the document existed at the indicated time.

Communication Manager uses digital certificates 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 files before installation. If the authentication or certificates do not match, the installation either fails or, in some cases, the system displays a warning 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.

Related Topics

- Avaya Public Key Infrastructure on page 63
- Secure updates of Avaya software and firmware on page 157

Secure administration

Access profiles

Use the System Management Interface (SMI) and the system access terminal (SAT) to gain access to Communication Manager, the underlying operating system, and the hardware components. For example, gateways and IP telephones.:

- With System Management Interface, you can:
  - Gain access to system alarms, logs, diagnostics.
  - Configure and monitor the security aspects of the system.
- The SAT interface provides access and functionality similar to the SMI and in-depth administration, diagnostics, and reports for the Communication Manager system.

Examples of in-depth administration include parameters for call routing patterns and coverage, stations, trunks, signaling groups, and network regions. Note that the user cannot gain access to the Linux operating system through the SAT interface.

Default login accounts that grants access to the SMI and the SAT screens are similar as the login accounts use numbered user profiles. The numbered user profiles usually correspond to Role-Based Access Control (RBAC). The interfaces and the account names of SMI and SAT are different.

For more information about profiles and default permissions for SMI and SAT interfaces, see:

- System Management Interface default profiles and permissions on page 32
- Communication Manager default SAT profiles and permissions on page 33

System Management Interface default profiles and permissions

System Management Interface profiles

The table on page 32 lists and describes the intended use of the default profiles for the System Management Interface.

Note:

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

Table 4: Communication Manager System Management Interface default profiles(continued)

Profilen umber	Group	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.
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

System Management Interface default settings

You can administer and configure access permissions to the System Management Interface on the **Security** > **Web Access Mask** page.

You must use the following two profiles as the bases for new user profiles, adding or restricting permissions to pages in accordance with the role-based access controls (RBAC) of the customer or individual security policy.

- **Profile 18** (superuser): With Profile 18, you can gain access to all the components of the System Management Interface screen. Use this profile as the basis for telephony administrators who must gain access to all of the SMI features. You must remove permissions from this profile as necessary when creating new superuser profiles.
- **Profile 19** (user): With Profile 19, you can gain access to fewer System Management Interface components. Use this profile as the basis for telephony administrators who need lower-level access to some of the SMI features. Add permissions from this profile as necessary when creating new user profiles.

Communication Manager default SAT profiles and permissions

Communication Manager default SAT profiles

The table on page 33 lists and describes the default profiles for the SAT interface.

Note:

Coresident applications such as Avaya Aura® Communication Manager Messaging or Octel voice mail adjuncts require a standard profile to support TSC access to Communication Manager.

Table 5: Communication Manager default SAT profiles

Profilen umber	Profile name	Permissions/access	Notes
0	Services superuser	Equivalent to the former SAT *init* login. Has all permissions possible with no restrictions.	Cannot be edited, copied, viewed, or removed. Restricted Requires a second user authentication by Communication Manager.
1	Services manager	Equivalent to the former SAT *inads* login	Cannot be edited, copied, viewed, or removed. Requires a second user authentication by Communication Manager.
2	Business Partner	Equivalent to the former SAT *dadmin* login	Cannot be edited, copied, viewed, or removed. Must be enabled in the license file.

Profilen umber	Profile name	Permissions/access	Notes
			The dadmin login can create one login that has craft login permissions and a name other than craft. The second craft login uses Profile 3 and can login without a second challenge.
3	Services	Equivalent to the former SAT *craft* login	Cannot be edited, copied, viewed, or removed. Requires a second user authentication by Communication Manager.
4-15		Reserved for future use by Avaya.	Cannot be edited, copied, viewed, or removed.
16	Call Center manager	Equivalent to the former SAT MIS login (@MIS) CMS/CCR access	Cannot be edited, copied, viewed, or removed. Assign CMS/CCR logins through the MIS application. Note, this is not a “user” login.
17	SNMP	SNMP agent access	Cannot be edited, copied, viewed, or removed.
18	Customer superuser	Equivalent to the former SAT default *customer super-user* login	Cannot be edited or removed.
19	Customer user	Equivalent to the former SAT default *non-super-user customer* login	This profile is used during upgrades only. This profile has no SAT permissions and cannot be edited or removed.
20-69		Available for customer modification	Use these profile numbers for customized permissions or role-based access control (RBAC).

Communication Manager profile default settings

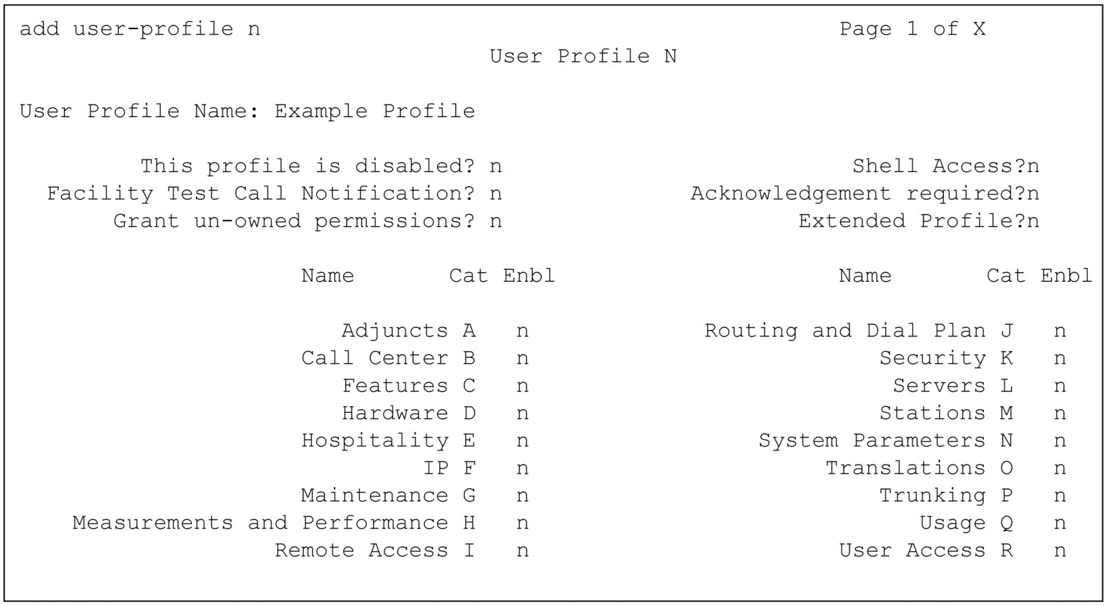
The **User Profile** form creates user profiles 20-69 and enables SAT permissions by lettered categories. Each category is associated with a unique set of SAT commands and forms designed to support role-based access control (RBAC) and segmented administration, maintenance, and monitoring.

Adding a new SAT profile

Procedure

At the SAT interface, type **`add user-profile n,`** where **`n`** is the new profile number, which may range from 20 to 69, to add a new SAT profile and administer profile permissions.

The **Cat** field lists categories in alphabetic order with a brief description in the **Name** field. In the **Enbl**field, the default setting is **n** for each category indicating that the access permissions are disabled.



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

User Profile Name: Example Profile

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

                     Name       Cat Enbl                     Name       Cat Enbl

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

Figure 4: Add a new SAT profile

Privilege escalation

Technicians who need higher privileges must log in using normal service accounts and then escalate 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.

The system logs the entries for privilege escalation and superuser activities in the following folders:

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

Reading superuser permissions and restrictions

About this task

Use this procedure to read superuser permissions and restrictions.

Procedure

Type **sudo -l** at the server CLI.

The system provides a list of commands that you are permitted to execute. The system also provides a list of commands that you can execute to escalate your profile to the superuser level.

Related topics:

Credentials complexity and expiration requirements on page 76
Managing Communication Manager accounts on page 83
Administration of authentication passwords on page 84

Local host account authentication

By default, Communication Manager supports only local host accounts as shown in the figure on page 36. In a local host account, the authentication, authorization, and accounting information is maintained on the same server that the user attempts to access.

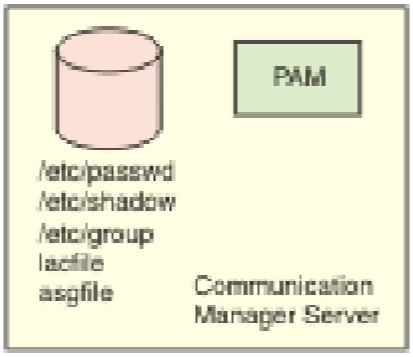


Figure 5: Local host accounts on the Communication Manager server

To prevent a system lockout, you must 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. You can use local host accounts at the same time as any of the other external AAA services. The local host configuration on Communication Manager uses the /etc/passwd, /etc/shadow, and /etc/group files, among others.

Chapter 3: Configurable Security

Encryption overview

Digital encryption eliminates the risk of exposing critical data in telephone conversations, voice mail, and signaling messages. A digital telephone call consists of voice data also called as bearer data and call signaling messages also called as control messages. Bearer data and signaling data pass through many devices and networks, sometimes over different networks or virtual paths. Without encrypting both data types, anyone with access to the networks and devices can intercept the following:

- Digitized voice signals in telephone calls and voice mail
- Call signaling messages that can:
    - Set up, maintain, and tear down calls
    - Contain call duration
    - Reveal the names and numbers of the callers
    - Transmit encryption keys
- Translation or administration data in transit to or saved on a storage device. This data can 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

The table on page 37 compares how encryption mitigates the vulnerabilities in signaling and bearer type of data.

.

Table 6: 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 implements cryptographic algorithms and methodologies that are generally accepted in the INFOSEC community. Additionally, the selected cryptographic functions must have the capability to be approved under an FIPS-140-2 or Common Criteria certification assessment.

The figure on page 38 shows the encrypted links in a Communication Manager enterprise.

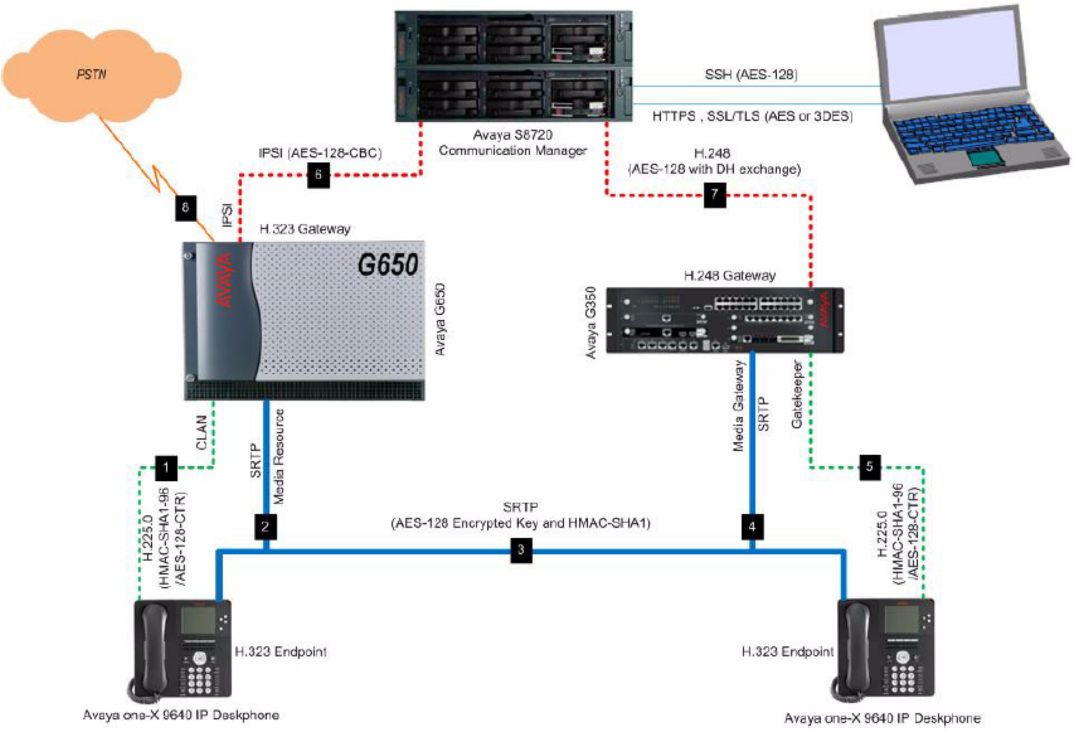


Figure 6: Encrypted links in Communication Manager enterprise

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

- IPSI link security on page 39 (Note 6)
- H.248 link security on page 39 (Note 7)
- H.225.0 Registration, Admission, and Status (RAS) on page 39 and H.225.0 call signaling on page 40 (Notes 1 and 5)
- RTP encryption on page 40 (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 and the Communication Manager server. In the signaling function, the IPSI link is also a conduit between the logical “gatekeeper,” resident in the Communication Manager server, and the H.323 endpoint through the central gateway.

To prevent unauthorized access or modification, the IPSI link is secured using the AES-128-CBC [AES] encryption algorithm. Inside the encrypted payload, the CRC-16 algorithm is used to detect errors and to prevent unauthorized modification of the payload. The IPSI link is only between two entities, an interface card and the Communication Manager server, therefore the key that is used to secure the IPSI link must be known only to the two entities. Since AES-128-CBC depends on the previous ciphertext block and the current plaintext, it is unlikely that a cycle of any length is identical unless the transmitted information is identical.--chk

H.248 link security

The H.248 link is the data link for control data between the gateway controller (the Communication Manager server) and H.248 branch gateways, (the Avaya G250, G350, G430, G450, TGM550 and G700 branch gateways) through the Gateway Control Protocol. The AES encryption algorithm protects data traversing this H.248 link and also includes a simple manipulation detection mechanism, an 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, the key remains resident in the volatile memory of the server and gateway, and is inaccessible by users or administrators. Since the key is stored in volatile memory, the key is destroyed whenever the H.248 link is re-created or whenever the server or gateway is turned off.

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

Before an H.323 IP endpoint can make a call, the endpoint 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, such as the endpoint 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 authenticating registration messages as well as encrypting and authenticating signaling messages. This ensures a secure registration process because it uses the HMAC-SHA1 authentication algorithm combined with an encrypted DH key exchange.

Since the keys are negotiated each time the endpoint registers, the keys are retained only in endpoint and gatekeeper RAM and are inaccessible by users or administrators.

H.225.0 call signaling

After the endpoint successfully registers, a second H.225.0 signaling link that transmits call-signaling messages is established between the gatekeeper and the endpoint. Examples of call-signaling messages include button presses, status indicators, and transmission of encryption keys when calls are established.

The signaling channel provides authentication of each packet using the standard HMAC-SHA1-96 algorithm and data encryption. Packets with 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 inaccessible by users or administrators. New session keys are created whenever the endpoints re-register.

RTP encryption

Avaya supports the following three encryption algorithms, all based on RFC3711:

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

For SRTP to work correctly, you must first enable SRTP, and administer SRTP using the administrative tools that Communication Manager provides.

Symmetric encryption keys that are generated dynamically are used for encrypting bearer traffic, also called as voice data. Any redirection in the RTP stream generates a new symmetric encryption key that is encrypted and sent from Communication Manager to H.323 endpoints. In addition to supporting H.235.5 for signaling encryption to the IP telephones, Avaya also support a challenge-response authentication method that generates a 56-bit DES encryption key to secure the encryption keys that are distributed to the H.323 IP endpoints.

SRTP is used with AES 128-bit encryption key and Avaya supports HMAC-SHA1-80 or HMAC-SHA1-32 based on the preference of the customer for authentication and integrity for each packet.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. SRTP for SIP uses RFC 4568 “Session Description Protocol (SDP) Security Descriptions for Streams” to distribute the encryption keys. 96xx SIP telephones establish a TLS connection to the Avaya Session Manager server using 128-bit AES encryption, and Session Manager communicates with Communication Manager using a 128-bit, AES-encrypted, TLS connection.

In all of these encryption solutions, the encryption keys are dynamically created for every connection. The keys are created within the gatekeeper and transmitted to the endpoints and processing boards over the secure links. Additionally, the system generates separate keys 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, the system generates additional keys to authenticate the RTP and RTCP (SRTP) messages.

All of these encryption keys are dynamically created and stored in RAM, and are inaccessible by administrators or users. The 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) streams are encrypted with 128-bit Diffie-Hellman and fixed symmetric keys. Whenever a stream starts or is re-configured, the keys are re-keyed or changed. The average cycle length for AES/SRTP with AES-128-CBC is reported to be 2^{127}, which is too long for a hacker to decrypt. Avaya uses a 128-bit block size 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. Therefore, it is unlikely that a cycle of any length is visible unless the transmitted information is identical.

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

Table 7: 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)

Encryption Technique	Available algorithms	Description
		information. Use this option to encrypt the following link: 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. AEA is not as secure as AES, but call capacity reduction with AEA is negligible.
SRTP		SRTP provides encryption and authentication of RTP streams for calls between SIP-SIP endpoints, H.323-H.323 endpoints, and SIP-H.323 endpoints. SIP endpoints cannot use AEA or AES encryption.
	1-srtp-aescm128-hmac80	Encrypted/Authenticated RTP with 80-bit authentication tag
	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

Branch gateway support

Table 8: Encryption supported in Avaya branch gateways

Model	Version	Supported encryption algorithms
TN2302AP (Medpro)	N/A	Supports AEA or AES • Extra DSP utilization using AES variant. AES reduces circuit-switched-to-IP call capacity by 25%. **Note:** For more information, see *Administering Network Connectivity on Avaya Aura® Communication Manager.*
TN2602AP (IP Resource 320)	SRTP support	Supports AEA or AES, and SRTP. Does not use “extra DSPs” for either method chosen.
TN2312BP (IPSI)		AES-128-Cipher Block Chaining
H.248 Branch Gateways (G350, G450, G430, G250)		Supports AEA or AES (128-Output FeedBack), and SRTP • Extra DSP Utilization using Avaya Encryption AES variant (differs based on the type of Branch Gateway) • Extra DSP utilization using SRTP

Deskphones and client endpoint support

Table 9: 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 Encryption

Model	Version	Detail
Avaya one-X Quick Edition	N/A	Does not support Avaya Encryption or SRTP
Avaya 3606, 3616, 3620, 3626, 3641, 3645 IP Wireless telephones (VoWLAN)	N/A	Does not support any form of Encryption
Avaya 3631 IP Wireless telephone (VoWLAN)	N/A	Supports AES
Avaya IP DECT (3711)	N/A	Does not support any form of Encryption
Avaya 46xx (H.323)	See the table on page 44.	Supports AEA or AES
Avaya 46xx (SIP firmware)	N/A	Does not support any form of Encryption
Avaya 4690 (H.323)	Requires firmware version 1.2 or greater	Supports AES
Avaya 96xx (H.323)	Firmware version 1.2 or greater	Supports AES Supports SRTP
Avaya 96xx (SIP firmware)Avaya 9620 Avaya 9630/G Avaya 9640/G	Requires firmware version 1.0 or greater Requires firmware version 2.0	Supports SRTP
Avaya 16xx one-X Deskphones	N/A	Supports AES

Table 10: Avaya 46XX IP telephone firmware versions supporting encryption

46XX telephone	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 telephone firmware or greater
Avaya 4610SW	Requires R2.3 telephone firmware or greater
Avaya 4620 Avaya 4620SW	Requires R2.3 telephone firmware or greater

46XX telephone	Description
Avaya 4621SW	Requires R2.3 telephone firmware or greater
Avaya 4622SW	Requires R2.3 telephone firmware or greater
Avaya 4625SW	Requires R2.7 telephone firmware or greater

Interaction of encryption with Communication Manager features

When a call is encrypted, some Communication Manager features and adjuncts remain unaffected except for the features and adjuncts listed in the table on page 45.

Table 11: 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 the call is sent to a voice messaging system. When the TN2302AP IP Processor circuit pack receives the encrypted voice stream, the circuit pack decrypts the packets before sending the packets to the voice messaging system, which then unencrypts and stores the packets.
Hairpinning	Hairpinning is not supported when one or both streams are encrypted, and Communication Manager does not request hairpinning on these encrypted connections.
VPN	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	The encryption performance varies based on the following conditions at call setup: • 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 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 clear text.

Table 12: H.248 gateways encryption interactions with Communication Manager features

Interaction Description	Description
VPN IPSEC	DES-SBC (56-bit) TDES-CBC (168-bit) AES-CBC (128-bit)
SSH2 server	DH (768-2048 bit) TDES-CBC (168 bit) DES-CBC (56-bit) RSA 1024, 2048 DSA 1024, 2048 AES 128 CBC
SNMPv3 agent	DES-CBC (56-bit) HMAC-SHA-1-96 HMAC-MD5-96 AES-CBC (128-bit)
RTP encryption	AES-CBC (128-bit)
Firmware Download Verification	RSA (1024-bit) decryption with SHA-1
License verification	Use RSA (1024-bit) decryption with SHA-1
IP telephony registration	The authentication mechanism is part of H.225 (RAS) registration of IP voice stations to survivable engine. The authentication uses 56-bit DES encryption of challenge token with station password (PIN) as the encryption key.
The TLS client	TDES-CBC, AES-CBC (128, 192, 256 bit).
Secure backup/restore	AES-CBC (128 bit), HMAC-SHA1-32 SRTP: AES-Avaya Aura® 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 the keys are overwritten whenever the links are disabled or re-created. Additionally, all links support the use of the AES encryption algorithm using 128-bit keys. When authentication is used, the HMAC-SHA1-96 authentication algorithm is implemented.

The table on page 47 shows that Communication Manager operations are secured from end-to-end using standard encryption and authentication algorithms and key negotiation.

Table 13: Communication Manager secure protocols

Link	Description	Transportprotocol	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 in the volatile memory of the gateway until the H.248 link is re-created or whenever the server or gateway is turned off. Users and administrators cannot access these 128-bit keys.
H.225.0	H.323 IP endpoint to gateway; endpoint authentication credentials not exposed.	RAS	HMAC-SHA1-96 AES-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 the RAM of the IP endpoint and gatekeeper and are inaccessible by users or administrators.
H.225.0	Signaling between gatekeeper and IP endpoint (for example,	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

Link	Description	Transportprotocol	Encryption / authentication algorithm	Key exchange
	button presses, status indicators, and transmission of encryption keys)			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 inaccessible by users or administrators.
RTP	Bearer traffic (voice calls)	SRTP	AES HMAC-SHA1	Keys are dynamically created for every connection. Separate keys are generated for the “transmit” and “receive” streams of each call. Keys are not escrowed but are stored in RAM where the keys are inaccessible by administrators or users. In conference calls, a unique key pair (one for transmit, one for receive) is assigned for encrypting the payload of each endpoint participating in the conference.
Administrative access	SAT interface for server to computer/ laptop	SSH	AES-128	SSH client on personal computer of the administrator negotiates with the server to determine which cipher suite is used. Keys are negotiated each time a link is established and the key is

Link	Description	Transportprotocol	Encryption / authentication algorithm	Key exchange
				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 are negotiated each time a link is established and the key is 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 Avaya Aura® CM software but inaccessible by users or administrators exchanged with 128-bit Diffie-Hellman. Since the IPSI link is only between a specific interface card and the server, the key that is used to secure the IPSI link must be known to only the two entities.
Account information	Required local account stored on 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.	SCP	AES-128	15-256 character pass phrase

Link	Description	Transportprotocol	Encryption / authentication algorithm	Key exchange
	For manual movement to another server running the same Communication Manager release.			

Additional information on secure communication

- [AES] Advanced Encryption Standard, FIPS-197, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
- [DH] W. Diffie and M.E. Hellman, “New Directions in Cryptography,” IEEE Transactions in Information Theory, v. IT-22, n. 6, Nov 1976, p. 664-654
- [EKE] Bellovin and Merritt, U.S. Patent 5,241,599, August 31, 1993, assigned to Lucent Technologies, AT&T Bell Laboratories.
- [GNUPG] www.gnupg.org
- [HMAC] H. Krawczyk, M. Bellare, and R. Canetti, HMAC: Keyed-Hashing for Message Authentication,
- IETF Informational RFC 2104, February 1997.
- [HTTPS] E. Rescorla; “HTTP over TLS”; RFC 2818, http://www.ietf.org/rfc/rfc2818.txt
- [ITUH2250] ITU-T Recommendation H.225.0, “Call signaling protocols and stream packetization for packet-based multicommunication systems.”
- [ITUH235H] ITU-T H.235 Amendment 1, “Security and encryption for H-series (H.323 and other H.245-based) multiterminals,” 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

Encryption administration in Avaya solutions

You must use the System Access Terminal (SAT) to administer encryption in Communication Manager CODEC (COder-DECoder) sets, network regions, and signaling groups.

The Administer encryption for IP CODEC sets through SAT on page 51 section explains how to assign an encryption algorithm to each supported CODEC. Communication Manager applies the encryption policy of the assigned CODEC to all IP endpoints in a network region.

The Administering encryption for signaling groups through SAT section explains how to enable encryption for IP signaling groups.

Administer encryption for IP CODEC sets through SAT

In order to administer encryption in Communication Manager, you need to assign an encryption algorithm to a CODEC set followed by assigning codecs to network regions.

Assigning an encryption algorithm to a CODEC set

Procedure

1. On the SAT screen, type **`change ip-codec-set n`**, where *n* is the number of the IP CODEC set.
2. In the Audio Codec column, enter the CODEC set number. To view a list of CODEC sets available in Communication Manager, type list ip-codec-set on the SAT screen.
3. In the Encryption column, enter the encryption algorithm.

   The system displays the Encryption column on the IP Codec Set screen only when the **Encryption** field on the Customer Options screen is set to **y** and the Encryption over IP feature is enabled in the license file.

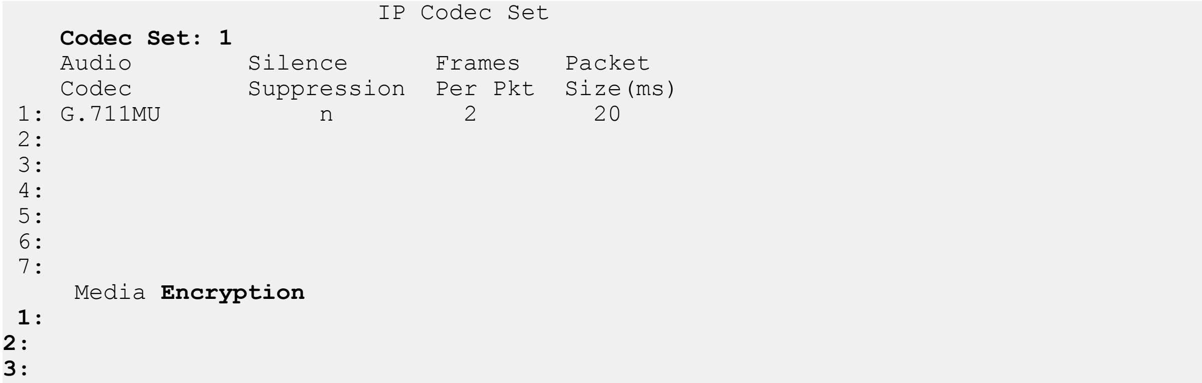
   The available encryption algorithms are listed and described in *Communication Manager administrable encryption algorithms*.

   Important:

   SRTP Encryption is supported by 96xx telephones only.

Result

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



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

Assigning CODECs to network regions

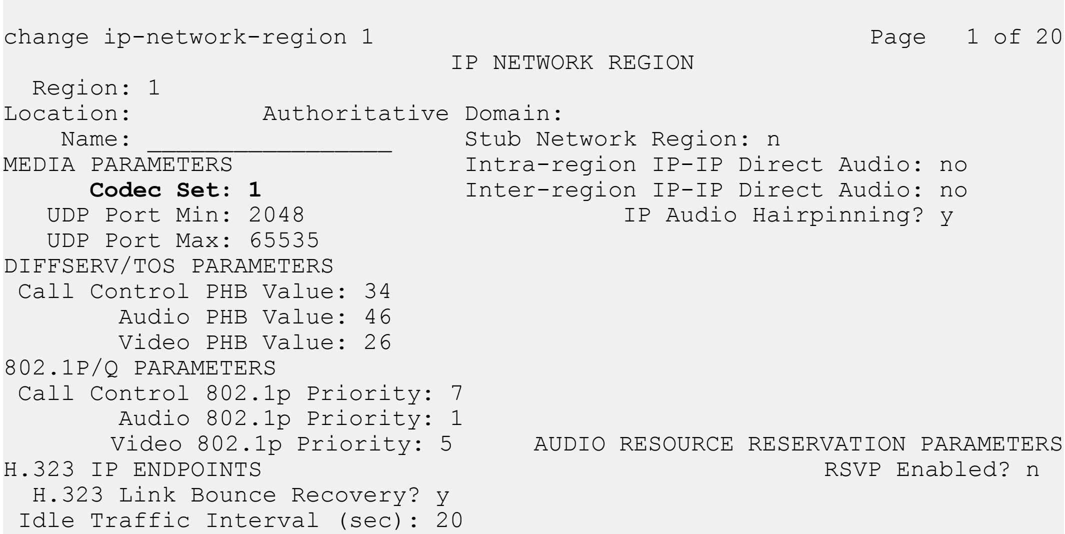
About this task

The second part of administering encryption in Communication Manager involves assigning CODECs to network regions. After administering the encryption algorithm, you must administer the CODEC set in the **IP Network Region** screen. This encryption algorithm is applicable to all the IP endpoints within the network region.

Procedure

1. On the SAT screen, type change ip-network-region n, where n is the network region number.
2. In the **Codec Set** field, enter the CODEC set that you administered in the **IP CODEC Set** screen.

   To administer a combination of encrypted and nonencrypted policies across multiple network regions, see Encrypted and nonencrypted policies on page 55.



```
change ip-network-region 1                                  Page   1 of 20
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain:
    Name: _________________     Stub Network Region: n
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
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 34
        Audio PHB Value: 46
        Video PHB Value: 26
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
 Idle Traffic Interval (sec): 20
```

```
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Communication Manager administrable encryption algorithms

Table 14: Communication Manager administrable encryption algorithms

Valid 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 the following links: • Server-to-gateway (H.248) • Gateway-to-endpoint (H.323)
aea	Avaya Encryption Algorithm. Use this option as an alternative to AES encryption when: • All endpoints within a network region using this codec set must be encrypted. • All endpoints communicating between two network regions and administered to use this codec set must be encrypted.
1-srtp-aescm128-hmac32	Encrypted/Authenticated RTP with 32-bit authentication tag
2-srtp-aescm128-hmac80 **Note:** The only supported SRTP value for stations is **srtp-aescm128-hmac80**. H.323 IP trunks support all eight of the listed SRTP algorithms.	Encrypted/Authenticated RTP with 80-bit authentication tag
3-srtp-aescm128-hmac32-unauth	Encrypted RTP but not authenticated
4-srtp-aescm128-hmac80-unauth	Encrypted RTP but not authenticated
5-srtp-aescm128-hmac32-unenc	Authenticated RTP with 32-bit authentication tag but not encrypted
6-srtp-aescm128-hmac80-unenc	Authenticated RTP with 80-bit authentication tag but not encrypted
7-srtp-aescm128-hmac32-unenc-unauth	Unencrypted/Unauthenticated RTP

Valid Encryption entries	Usage
8-srtp-aescm128-hmac80-unenc-unauth	Unencrypted/Unauthenticated RTP
none	stream is unencrypted (default)

Administering encryption for signaling groups through SAT

About this task

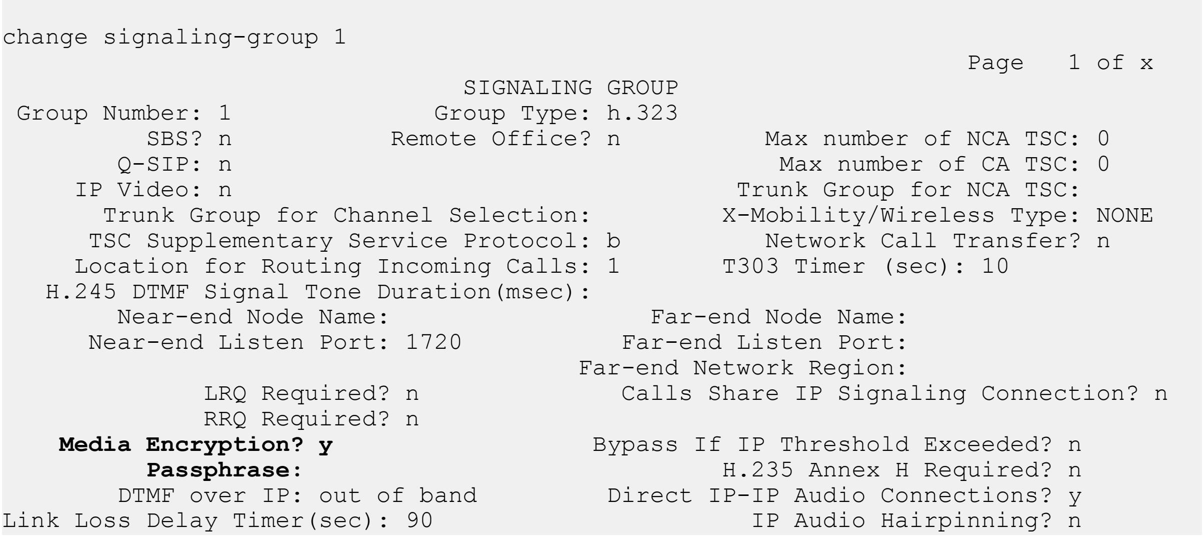
To administer encryption for signaling groups in Communication Manager, you must enable encryption on the **Signaling Group** form.

Procedure

1. On the SAT screen, type change signaling-group n, where n is the signaling group number.
2. Set the **Media Encryption** field to **y**. The system displays the **Media Encryption** field on the **Signaling Group** screen only when the **Encryption** field on the **Customer Options** screen is set to **y** and the **Encryption over IP** feature is enabled in the license file.
3. In the **Passphrase** field, enter a string that has a maximum length of 30 characters.

Result

For more information on signaling group encryption and caveats regarding end-to-end trunk and passphrase administration, see *Administering Network Connectivity on Avaya Aura® Communication Manager*.



```
change signaling-group 1
                                                                   Page   1 of x
                                SIGNALING GROUP
 Group Number: 1              Group Type: h.323
          SBS? n           Remote Office? n          Max number of NCA TSC: 0
        Q-SIP: n                                      Max number of CA TSC: 0
     IP Video: n                                   Trunk Group for NCA TSC:
       Trunk Group for Channel Selection:         X-Mobility/Wireless Type: NONE
      TSC Supplementary Service Protocol: b          Network Call Transfer? n
     Location for Routing Incoming Calls: 1       T303 Timer (sec): 10
   H.245 DTMF Signal Tone Duration(msec):
        Near-end Node Name:                   Far-end Node Name:
      Near-end Listen Port: 1720            Far-end Listen Port:
                                        Far-end Network Region:
              LRQ Required? n               Calls Share IP Signaling Connection? n
              RRQ Required? n
    Media Encryption? y                   Bypass If IP Threshold Exceeded? n
          Passphrase:                            H.235 Annex H Required? n
        DTMF over IP: out of band        Direct IP-IP Audio Connections? y
Link Loss Delay Timer(sec): 90                     IP Audio Hairpinning? n
```

```
       Enable Layer 3 Test? n                   Interworking Message: PROGress
H.323 Station Outgoing Direct Media? n   DCP/Analog Bearer Capability: 3.1kHz
```

Additional information on encryption

- Encrypted and nonencrypted policies on page 55.
- “Administering IP network regions” and “Administering 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.
- For more information on encryption in relation to Communication Manager, download the “Configuring Avaya Communication Manager for Encryption,” whitepaper from http://www.avaya.com/master-usa/en-us/resource/assets/applicationnotes/media-encrypt.pdf.

Encrypted and nonencrypted policies

The section Encryption administration in Avaya solutions on page 51 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 a separate encryption scheme, then interconnecting the regions can apply encrypted and nonencrypted policies across the enterprise.

For more information about administering network regions, including topics related to interconnecting regions with disparate provisioning, see *Administering Network Connectivity on Avaya Aura® Communication Manager, 555-233-504*. This guide provides more information about administering network region connectivity, 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 on encryption administration

- Encryption administration in Avaya solutions on page 51
- 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 Aura® Solution Design Considerations and Guidelines*, 03-603978

Authentication files for Communication Manager

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

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

You must create and install a new authentication file whenever you upgrade Communication Manager to a new major release.

Important:

Installing the authentication files also installs the Avaya digital certificate for Communication Manager.

Authentication files for duplicated servers and survivable servers

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

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

Authentication file

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

Each authentication file is identified with an authentication file ID (AFID). You need this AFID to create a new authentication file for an upgrade or to replace the current authentication file on the server.

Avaya Security Gateway

Avaya Security Gateway (ASG) is a challenge-response mechanism that replaces the use of passwords. When a user attempts to log in to an ASG-enabled account on the server, the system displays a randomly generated number instead of a request for a password. The user must use a tool such as ASG Web Mobile to obtain the appropriate response to the challenge. Users are permitted to log in only if they enter the correct response.

Starting the Authentication File System application

About this task

AFS is available only to Avaya and Avaya Partners. If you are a customer and need an authentication file, log on to the Avaya Support website at http://support.avaya.com for current documentation, product notices, knowledge articles related to the topic, or to open a service request.

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

Procedure

1. Type http://rfa.avaya.com in your Web browser.
2. Enter your login information and click **Submit**.
3. Click **Start the AFS Application**.The system displays a security message.
4. Click **I agree**. The system starts the AFS application.

Creating an authentication file for a new system

About this task

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

Procedure

1. Log on to the AFS application.
2. In the **Product** field, select **SP System Platform**.
3. In the **Release** field, select the release number of the software, and click **Next**.
4. Select **New System**, and then click **Next**.
5. Enter the fully qualified domain name (FQDN) of the host system where Communication Manager is installed. For duplicated Communication Manager servers, enter the alias FQDN.
6. Enter the FQDN of the Utility Server.
7. To download the authentication file from the AFS application to your computer:
    a. Click **Download file to my Personal Computer**.
    b. Click **Save** in the File Download dialog box.
    c. Select the location to save the authentication file, and click **Save**.
    d. After the download is complete, click **Close** in the Download complete dialog box. After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).
8. To receive the authentication file in an email message:
    a. Enter the email address in the **Email Address** field.
    b. Click **Download file via email**. AFS sends the e-mail message that includes the authentication file as an attachment and the AFID, system type, and release in the message text.
    c. Save the authentication file on the local computer. After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).
9. You can use WordPad to open the authentication file and view the header information in the authentication file. The header includes the AFID, product name and release number, and the date and time the authentication file was generated.

Creating an authentication file for a file replacement

Before you begin

You must have the AFID of the authentication file to replace. See Obtaining the AFID from System Platform Web console on page 61 or Obtaining the AFID from Communication Manager SMI on page 61.

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

Procedure

1. Log on to the AFS application.
2. In the **Product** field, select **SP System Platform.**
3. In the **Release** field, select the release number of the software, and then click **Next**.
4. Select **Upgrade or Re-deliver for Existing System**.
5. In the **Authentication File ID** field, enter the AFID for the authentication file that is currently installed on the system, and then click **Next**.
6. Select one of the following options:
   - If you use an Avaya Services login to access Communication Manager, read the product access instructions, and select **I read and understand the Product Access Instructions**.
   - If you do not use an Avaya Services login to access Communication Manager, select **I do not use Avaya Services logins**.
7. To download the authentication file from the AFS application to your computer:
   a. Click **Download file to my Personal Computer**.
   b. Click **Save** in the File Download dialog box.
   c. Select the location to save the authentication file, and then click **Save**. After the download is complete, click **Close** in the Download complete dialog box. After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).
8. To receive the authentication file in an email message:
   a. Enter the e-mail address in the **Email Address** field.
   b. Click **Download file via email**. AFS sends the email message that includes the authentication file as an attachment and the AFID, system type, and release in the message text.
   c. Save the authentication file to the local computer. After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).

9. You can use WordPad to open the authentication file and view the header information in the authentication file. The header includes the AFID, product name and release number, and the date and time that the authentication file was generated.

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

About this task

Prerequisites

You must have the AFID of the authentication file on the system that you are upgrading. See Obtaining the AFID from System Platform Web console on page 61 or Obtaining the AFID from Communication Manager SMI on page 61.

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

Procedure

1. Log on to the AFS application.
2. In the **Product** field, select **SP System Platform**.
3. In the **Release** field, select the release number of the software to which you are upgrading, and then click **Next**.
4. Select **Upgrade or Re-deliver for Existing System**.
5. In the **Authentication File ID** field, enter the AFID for the authentication file that is currently installed on the system, and then click **Next**.
6. Select one of the following options:
   - If you use an Avaya Services login to access Communication Manager, read the product access instructions, and select **I read and understand the Product Access Instructions**.
   - If you do not use an Avaya Services login to access Communication Manager, select **I do not use Avaya Services logins**.
7. To download the authentication file from the AFS application to your computer:
   a. Click **Download file to my Personal Computer**.
   b. Click **Save** in the File Download dialog box.
   c. Select the location to save the authentication file, and then click **Save**.
   d. After the download is complete, click **Close** in the Download complete dialog box. After the authentication file is created, AFS displays a confirmation

message that contains the system type, release, and authentication file ID (AFID).

8. To receive the authentication file sent in an email message:
    a. Enter the e-mail address in the **Email Address** field.
    b. Click **Download file via email**. AFS sends the e-mail message that includes the authentication file as an attachment and the AFID, system type, and release in the message text.
    c. Save the authentication file to the local computer. After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).
9. You can use WordPad to open the authentication file and view the header information in the authentication file. The header includes the AFID, product name and release number, and the date and time that the authentication file was generated.

Obtaining the AFID from System Platform Web console

Procedure

1. Log on to the System Platform Web Console.
2. In the navigation pane, click **User Administration** > **Authentication File**.

    The system displays the AFID in the **AFID** field. An AFID of 7100000000 is the default authentication that is installed with System Platform. The default file must be replaced with a unique file.

Obtaining the AFID from Communication Manager SMI

Procedure

1. Log on to Communication Manager System Management Interface (SMI).
2. Click **Administration > Server (Maintenance)**.
3. In the navigation pane, click **Security** > **Authentication File**.

    The system displays the AFID in the **AFID** field. An AFID of 7100000000 is the default authentication that is installed with System Platform. The default file must be replaced with a unique file.

Installing an authentication file

Before you begin

You must create and download the authentication file from AFS.

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

Once the suser account is created, the authentication that is installed on System Platform.

Procedure

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

   Note:

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

   - You must install an authentication file that has a different AFID than the file that is currently installed
   - You have already installed a new authentication file, but must reinstall the original file. You must not select this option if you are replacing the default authentication file with a unique authentication file.

     Caution:

     Use caution when selecting the **Force load of new file** option. If you install the wrong authentication file, certificate errors and login issues might occur.
5. Click **Install**. The system uploads and validates the selected authentication file. After validation, the system installs the authentication file.
6. To confirm that the authentication file is installed on Communication Manager, check the Authentication File page from the SMI.

Digital certificates and server trust relationships

Chain of trust

Digital certificates certify the identity of the public-key owner. A trusted party signs the public key and the information about the owner, creating a public-key certificate. The certificate is similar to a driver's license that guarantees the identity of the owner.

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. The CA also can belong to the same organization as the entities the organization serves. CAs can issue certificates to other sub-CAs, which creates a tree-like certification hierarchy called a public-key infrastructure (PKI).

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

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

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

Avaya RFA uses a:

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

The secure hardware and daemon ensure that 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 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 infrastructure of the customer, including IP telephony.

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

- The sending process/person is actually the originator.
- The receiving process/person is the intended recipient.
- Data integrity is uncompromised.

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

The Avaya product PKI is limited to device-to-device authentication primarily to automatically establish a TLS or similar connection to ensure confidentiality, integrity, and authenticity. VoIP devices that use Avaya software or must establish a TLS connection with other devices 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 following:

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

The table on page 64 lists the Avaya public and private keys and their uses.

Table 15: Key pair and certificate usage

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

Note:

The Avaya Product Certificate Authority does perform the following:

- Publish subscriber certificates, but archives copies of certificates
- Notify other entities of certificates that the Authority has issued
- Issue certificates to individuals

Avaya security certificate types

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

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

A server certificate verifies the identity of a server. The server certificate changes every time the server is reconfigured. If the server name is changed, the customer gets a security alert the next time the customer attempts to log in.

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

The second server certificate is issued to a site-specific Avaya server such as, SIP-TLS and HTTPS. After the server certificate is configured, the certificate name is unique to that particular server of the site.

Important:

Before you can log in to the Avaya server, you must accept or store the server certificate.

Avaya certificate repository

Digital certificates in Communication Manager are stored in fixed directories called as certificate repositories.

PKI in Communication Manager

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

- Establish SIP/TLS connections between IP telephones and Communication Manager through the customer-installed, trusted, third-party certificate. For more information, see section Communication Manager trusted certificates on page 70.
- Establish connections between IP telephones and Communication Manager through the trusted chain of Avaya for the purpose of securing configuration downloads and firmware

updates to the IP telephone. For further information, see section PKI in H.323 and SIP endpoints on page 71.

- Download configuration data from Communication Manager for file synchronization. for more information, see section Filesync to duplicated or survivable servers on page 74.
- Authenticate access to the Communication Manager Web interface. For more information, see section, Connection to Communication Manager Web interface on page 74.
- SIP/TLS connections
    - Management
    - Signaling

Installing a Root Certificate on a Personal Computer

About this task

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

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

⚠ **Warning:**

You must install a CA certificate as a Root Certificate.

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

Procedure

1. Log in to Communication Manager System Management Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Security** > **Install Root Certificate**.
4. On the **Install Root Certificate** page, click **Install**.
5. In the **File Download - Security Warning** dialog box, click **Save**.
6. Select a location and save the file.
7. After the file is downloaded, locate the file and double-click the file.
8. In the **Open File - Security Warning** dialog box, click **Open**.
9. On the **General** tab in the **Certificate** dialog box, click **Install Certificate**.
10. Accept the default settings in the **Certificate Import Wizard**, and click **Finish**.

Trusted certificates

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

Displaying a trusted certificate on the server

Procedure

On the **Trusted Certificate** page, select a certificate entry, and click **Display**

Adding a trusted certificate to the server

Before you begin

Ensure that a trusted certificate must be a Certificate Authority (CA) certificate.

Procedure

1. On the **Trusted Certificates** page, click **Add**.
2. On the **Trusted Certificate-Add** page, enter the file name of the certificate that you want to add. The certificate that you want to add must be listed in a pem file*and* in the `/var/home/ftp/pub` directory.
3. To validate the certificate, click **Open**. The **Trusted Certificates – Add** page displays the issued-to, issued by, and expiration date information for the certificate. The system displays an error message if the certificate is invalid.
4. Enter a name of the certificate. Provide the same certificate name in all repositories.
5. Select the repositories where you want to add the certificate, and click **Add**. The system checks for the following:
   a. The certificate name has a `.crt` extension. If the certificate name has a different extension, the system replaces the extension with `.crt`.
   b. The certificate name is unique.
   c. The certificate is not a duplicate certificate with a new name.

Deleting a trusted certificate from the server

Procedure

1. On the **Trusted Certificate** page, select a certificate entry, and click **Remove**.
2. On the **Trusted Certificate - Remove** page, select the repositories you want the certificate deleted from, and click **Remove**.

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

Procedure

1. On the **Trusted Certificate** page, select a certificate entry, and click **Copy**.
2. On the **Trusted Certificates – Copy** page, select the repositories you want the certificate copied to, and click **Copy**.The system checks for the following:
   a. The certificate name is unique.
   b. The certificate is not a duplicate certificate with a new name.

   Note:

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

Server certificates and application certificates

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

Important:

You must update the server certificate every time you change the server name.

The Avaya server has two server certificates. One certificate is specific to the service technicians who log in to many servers. The service technician certificate is issued to the services Ethernet interface address, `192.11.13.6`, and identifies the certificate authority as the Avaya Call Server. The second certificate is specific to the site-specific server name.

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

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

Note:

One of the CAs in the server certificate must be a part of the Communication Manager trusted certificates repository.

Displaying a server certificate or application certificate

Procedure

1. From the **Server/Application Certificates** page, select a certificate and click **Display**.

2. Click **Back** from the **Server/Application Certificates - Display** page to return to the main **Server/Application Certificates** page.

Adding a server certificate or application certificate to the server

Before you begin

Communication Manager must include at least one corresponding Certificate Signing Request (CSR), or add a private key to the server certificate. To create a new CSR, use the **Certificate Signing Request-Form** on the **Security** tab of the Avaya Aura® Communication Manager System Management Interface. For online help, click the **Help** button on the SMI screen.

Important:

Log in with the `suser` credential to add a server or application certificate.

Procedure

1. On the **Server/Application Certificates** page, click **Add**.
2. From the **Server/Application Certificates-Add** page, enter the file name of a certificate in `/var/home/ftp/pub` that contains the certificate chain you must add. The certificate must be either a PKCS#12 file or a file in pem format.
3. If required, enter the password of the certificate.
4. To validate the certificate, click **Open**. The system displays the following information on the **Server/Application Certificates - Add** page:
    - *Issued to*
    - *Issued by*
    - *Date of Expiration*
5. Select the repositories where you want to install the certificates, and click **Add**.

    Note:

    The default file name of the certificate is `server.crt`. For a single server and application certificate chain, the server sub directory of a repository is limited to a single file for a single certificate chain. The file name is server.crt. This certificate represents the identity of only one server. The system overwrites any existing `server.crt` file with the new certificate.

Removing a server certificate or application certificate from the server

Before you begin

You must log in as an **suser** to add a server or application certificate.

Procedure

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

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

Before you begin

You must log in as an **suser** to add a server or application certificate.

Procedure

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

Communication Manager trusted certificates

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

Communication Manager loads the following trusted certificates present in the repository into the runtime memory of the server:

- 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.

To load a third-party trusted certificate into the Communication Manager repository, use the `tlscertmanage` command at the server command line. You must restart Communication Manager after installing the third-party trusted certificate. For more information, see section Additional information on digital certificate on page 76.

The **all-ca.crt** file can contain up to four (4) Communication Manager-related certificates and up to four (4) additional third-party certificates. If the **all-ca.crt** file contains more than eight certificates, Communication Manager loads only the first eight certificates, ignores the remaining certificates, and generates a minor alarm and adds an entry in the syslog file to notify the user about the error condition.

Third-party certificate management

The table on page 71 describes how Communication Manager handles third-party certificates.

Table 16: Communication Manager third-party certificate management

Activity	Description
File sync	To prevent overwriting a customer-installed, third-party certificate, file sync does not synchronize any certificates.
Upgrades	See Upgrading the third-party certificate on page 71.
Backup / restore	Backup and restore software does not back up or restore trusted certificates.

Upgrading the third-party certificate

Procedure

1. Copy the third-party certificate file to the server.
2. Type the **`tlscertmanage`** command to add the certificate to the trusted repository.
3. After the upgrade, reinstall the third-party certificate with the **`tlscertmanage`** command.

Note:

You must not delete the original certificate file. However, if the original file is deleted, you must copy the original certificate file from the source to the server.

PKI in H.323 and SIP endpoints

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

- Before upgrading firmware of IP telephones, Communication Manager validates the embedded certificate before downloading the firmware file to the IP telephone. You cannot view the embedded certificate from the telephone or any standard interface.
- Authenticates the Session Manager server (Avaya One-X 96XX SIP telephone only).

Note:

The firmware in the Avaya IP telephones does not verify whether the Communication Manager identity certificate has expired, but the firmware verifies the chain of trust for the incoming Communication Manager certificate.

IP telephones are typically provisioned in a staging area where the certificate authority and a Web server are on a physically-separated LAN. The IP telephones 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 telephones, you can use the certificates anywhere in an enterprise.

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

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

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

  Note:

  The CN in the telephone certificate is typically the telephone 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

Usage of certificates in Avaya endpoints

The table on page 72 lists the certificate usage in Avaya H.323 telephones (96XX, 46XX, and 16XX) and SIP telephones (Avaya One-X 96XX).

Table 17: Certificate usage in Avaya endpoints

Telephone type	Certificate	Use/Description
96XX (H.323)	Avaya Product Root Certificate Authority Trust Certificates **Note:** Beginning with 46XX H.323 Release 2.9 firmware and 96XX H.323 Release 2.0 firmware customers can import trusted third-party certificates	Download configuration files port trusted certificates **Note:** Includes 46xxsettings.txt, 46xxupgrade.scr, 96xxupgrade.txt, etc. downloaded through the

Telephone type	Certificate	Use/Description
	to the telephone using the TRUSTCERT parameter.	Communication Manager HTTPS server.
46XX (H.323)	Avaya Product Root Certificate Authority Trust Certificates **Note:** Beginning with 46XX H.323 Release 2.9 firmware and 96XX H.323 Release 2.0 firmware customers can import trusted third-party certificates to the telephone using the TRUSTCERT parameter.	Download configuration files Import trusted certificates **Note:** Includes 46xxsettings.txt, 46xxupgrade.scr, 96xxupgrade.txt, etc. downloaded through the Communication Manager HTTPS server.
16XX (H.323)	Avaya Product Root Certificate Authority	Download configuration files **Note:** Includes 46xxsettings.txt, 46xxupgrade.scr, 96xxupgrade.txt, etc. downloaded through the Communication Manager HTTPS server.
96XX SIP	Avaya Product Root Certificate Authority **Note:** Simple Object Access Protocol (SOAP) between the 96XX SIP telephones and Session Manager by default uses HTTP but can be configured for HTTPS, in which case the Avaya Product Root Certificate Authority (CA) certificate authenticates the Session Manager server through the signed CA identity certificate. x.509 Identity Certificate **Tip:** Customers can replace the default identify certificate using the Simple Certificate Enrollment Protocol (SCEP, see Additional information on digital certificate on page 76).	Download configuration files over HTTPS, when enabled. Establishes a SIP/TLS connection to the Avaya Session Manager server and used if 802.1X EAP/TLS is enabled. **Note:** Uses TLSSRVR, TSLPORT, HTTPSRVR, and HTTPPORT parameters in the DHCP Option #242. The TLS connection from the SIP telephone to the Session Manager server is encrypted using TLS_RSA_WITH_AES_128_CBC_SHA.
SIP Softphone	Hard-coded certificate	SIP Softphone firmware includes a default telephone certificate.

Telephone type	Certificate	Use/Description
		Note: Customers must use a uniquely-provisioned telephone certificate installed through Simple Certificate Enrollment Protocol (SCEP). For more information, see Additional information on digital certificate on page 76.

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 system accepts the certificate after the license installation is complete, and the server is fully operational. The server certificate is stored in `/etc/opt/ecs/certs/web443/ID` folder and requires root access to view the contents of the folder.

Filesync to duplicated or survivable servers

Duplicated Servers use filesync to send the server certificates from the active server to the standby server. 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 transmission.

Communication Manager also uses filesync to download configuration data to a Survivable Core Server for file synchronization.

Manage changes to the Avaya certificate

The table on page 74 lists how Avaya manages changes to digital certificates.

Table 18: 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.

Type of change	Description
Revocation	Certificates are revoked if the customer, technical support, or members of the Avaya Security Team believes the certificate has been compromised for any reason. Final decision is left to the Avaya Product Certificate Authority. A certificate is revoked in the following circumstances: • The information in the certificate is wrong or inaccurate. • The subject has failed to comply with the rules in the policy. • The system to which the certificate has been issued is no longer supported.
Who can request revocation?	The following entities or people can request certificate revocations: • The certificate subscriber • The Registration Authority (RA) that has performed the validation of the certificate request • Any entity presenting proof of responsibility for a certified Avaya SIP product • Any entity presenting proof of the certificate misuse • Any entity presenting proof of the private key compromise The final decision on revocation of the certificate is left to the Avaya Product Certificate Authority.
Procedure for revocation request	The Avaya Product Certificate Authority accepts revocation requests by e-mail only: apca@avaya.com. The e-mail must be authenticated and must include the serial number and subject name of the certificate in question.
Revocation request grace period	Avaya determines a timeframe for response at the time of the request.

Certificate alarms

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

The system automatically generates major alarms seven days before the certificate expires and also on the day the certificate expires on the server.

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

Creating certificate alarms

About this task

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

Procedure

1. On the **Avaya Aura Communication Manager System Management Interface (SMI)** page, select **Certificate Alarms**.
2. On the **Certificate Alarms** page, check one or all of the check boxes and perform the following:
    - Create a warning alarm or a minor alarm between 61 - 180 days before the certificate expires.
    - Create a warning alarm, a major alarm, or a minor alarm between 31 - 60 days before the certificate expires.
    - Create a major alarm or a minor alarm between 8 - 30 days before the certificate expires.
3. You must select the type of warning from the drop-down box, and the number of days the system must generate the alarm before the certificate expires.
4. Click **Submit**.

Additional information on digital certificate

- 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, Gateways and Servers, 03-300431*.
- Information about the alarm generated by incorrect third-party certificate administration is in *Maintenance Alarms for Avaya Aura® Communication Manager, Gateways and Servers, 03-300430*.

Administrative accounts

Credentials complexity and expiration requirements

Communication Manager logins comply with:

- Password complexity policies on page 77
- Credentials expiration and lockout policies on page 77

Password complexity policies

Password complexity rules that apply to passwords for local administrator and user accounts are listed in the table on page 77. Attempts to create disallowed passwords result in an instructive error message.

Table 19: Password complexity rules for Communication Manager

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

Password complexity rules that apply for the Branch Gateways are listed below:

Table 20: Password complexity rules for Branch Gateways

Password complexity rules	Parameters
Minimum length	Default is 6.
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**. This page sets global policy for all logins created through the **Server (Maintenance)** page. 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:

To manage credentials expiration and lockout policies for branch gateways, you must log in to gateways CLI.

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

- *Administration for the Avaya G250 and Avaya G350 Branch Gateways, 03-300436*
- *Administering Avaya G430 Branch Gateway*, 03-603228
- *Administering Avaya G450 Branch Gateway*, 03-602055

Field descriptions of the Login Account Policy page

The following table provides the description of the fields on the **Login Account Policy** page.

Name	Description
Credential Expiration Parameters	
The maximum number of days a password can be used (PASS_MAX_DAYS):	1-99999
The minimum number of days permitted between password changes (PASS_MIN_DAYS):	0-99999
The number of days a warning is given before a password expires (PASS_WARN_AGE):	0-30
The number of days after a password expires to lock the account (INACTIVE, 0= immediate, 99999=never):	0-99999 ✱ **Note:** 0 = immediate 99999 = never
Failed Login Response	
Enable account lock out parameters (PAM Tally)	If unchecked, the remaining parameters (below) are ignored.
Lock out account after the following number of unsuccessful attempts (DENY):	1-9
Automatically unlock a locked account after the following number of seconds (UNLOCK_TIME):	1-99999
Reset the failed attempt counter after last failed attempt (UNLOCK_RESET):	Yes or No

Password administration recommendations

The following recommendations and constraints can guide customers for Communication Manager password management:

- Although Avaya services might access your system at very infrequent intervals, you must disable password aging for all Avaya services accounts.
- For accounts that use an external server to authenticate passwords, such as RADIUS accounts, where users cannot use Communication Manager to change passwords, users must be careful while enabling password aging for such accounts.If such a user account expires, then the user is permanently locked out.

Credentials management

Credentials, such as usernames and passwords, for standard Linux accounts in Communication Manager are stored in `/etc/passwd`, `/etc/shadow`, and `/etc/group`, along with the backup of the credential files, for example, `/etc/group-` and `/etc/passwd-`.

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

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

Assign profiles for role-based administration

With role-based access control (RBAC), organizations can assign server, gateway, and application access permissions based on the job function or role of a user. 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 provide access to Avaya server and gateway information according to job functions and business needs. For more information on RBAC profiles, see the table on page 80.

Table 21: RBAC profile examples

Profile name	Job function and access permissions
Privileged Administrator	This login provides the greatest access to the system with the exception of the “root” login: read-write access to system parameters, such as IP addresses, software upgrades, modify, assign, or define other roles, and read/write access to create and modify logins. For procedures to set up this account, see Creating the privileged administrator account on page 80.
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

About this task

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

Procedure

1. On the **Administration** menu, click **Server (Maintenance) > Security > Administrator Accounts**.
2. Select **Add Login** and **Privileged Administrator**, click **Submit**.

   The system displays the **Administrator Accounts -- Add Login: Privileged Administrator** page.
3. Use the following table to fill in the appropriate fields.

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

Name	Description
Login name	Up to 31 characters (a-z, A-Z, 0-9). The login name must be unique and cannot be a protected login name. New or modified ASG customer protected logins require an AES key.
Primary group	Set to `susers` and cannot be changed.
Additional groups	The drop-down menu contains profiles 18 through 69. Profile 18 is the default.
Linux shell	Set to `/bin/bash` and cannot be changed.
Home directory	Updated automatically to `/var/home/`*`login-name`* when you enter the Login name. The entry cannot be changed.
Lock this account	Select this check box to lock the user from logging into the system. (Optional)
Date to disable	The date indicates when the login ID becomes disabled. The date must be in the *yyyy-mm-dd* format or blank (never disabled).
Type of authentication	• Password • ASG: Enter key (user defined, ASG user information must include the ASG key) • ASG: Auto-generate key (Avaya Aura® CM automatically generates the ASG key). If you select this option, the system deactivates the **Enter key or password** and **Re-enter key or password** fields.
Enter key or password	Field can be up to 31 characters and can include the following: • lowercase letters of the English alphabet (a-z) • uppercase or capital letters of the English alphabet (A-Z) • 0-9 • periods (.)

Name	Description
	• hyphens (-) • underscores (_) • dollar sign ($) • a blank space • colons (:) • semi-colons (;) • commas (,) • equal sign (=) • forward slash (/) • ampersand (&) • pound sign (#) • plus sign (+) • apostrophe (’) • asterisk (*) • quotation marks (“”) • parentheses(()) In previous releases of Communication Manager, the ASG key must be exactly 20 digits. Each digit must be an octal number, that is, between 0-7. The last digit must be zero ("0”) and the penultimate digit must be an even number. From Communication Manager 6.0, the ASG key is AES encrypted with a 32-digit key with hexadecimal characters.
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**.

Additional information on administering profiles

For information on administering profiles, you can download the following documents from the Avaya Support website at http://support.avaya.com.

- *Avaya Aura® Communication Manager Administrator Logins*.
- *Documentation for Avaya Aura® Communication Manager, Gateways and Servers* CD, and the following 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, Branch Gateway and Servers*, 03-300431
    - *Administration for the Avaya G250 and Avaya G350 Branch Gateway*s, 03-300436
    - *Administering Avaya G430 Branch Gateway*, 03-603228
    - *Administering Avaya G450 Branch Gateway*, 03-602055

Managing Communication Manager 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 the table on page 83. For more information, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Table 22: Managing Communication Manager accounts

Communication Manager account administration	Interface
Managing Avaya Server web interface login accounts • Adding an administrator account (login) • Changing, locking, removing logins • Adding and removing login groups	System Management Interface **Security** > **Administrator Accounts**
Managing Avaya server web access profiles • Adding web access profiles • Changing, duplicating, and deleting web profiles	System Management Interface **Security** > **Web Access Mask**
Managing passwords and Access Security Gateway (ASG)	System Management Interface **Security** > **Web Access Mask**

Communication Manager account administration	Interface
Managing profiles for SAT interface access • Adding a user profile for using the SAT • Adding extended profiles • Duplicating and deleting SAT profiles	SAT Screen **User Profile**

Account administration recommendations

Use the following recommendations and constraints for Communication Manager login account management:

- Administer at least one local host account in all servers so that getting access is possible even if external AAA servers are not reachable.
- Authenticate all ASG accounts to be local host accounts. A PAM module to support ASG authentication through an external server does not exist
- Disable password aging for all Avaya services accounts. Although, Avaya services might reach out to your system at very infrequent intervals to verify the same.
- Use RADIUS, RSA SecurID, and SafeWord AAA services with a parallel local host account or LDAP/NSS. When configuring a local host account, if the external AAA server is unreachable, lock the local account to prevent the use of a stale local password. The system does not support the Simple Authentication and Security Layer (SASL) authentication.

Administration of 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*.

Description of Access Security Gateway

Access Security Gateway (ASG) is a software feature available on most Avaya products and uses challenge/response for authentication by associating a unique secret key with each login on every product. When you install a new product, 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 is affected. The encryption keys are themselves encrypted before they are installed. ASG is session-oriented. A unique challenge is presented, and a unique response must be provided each time the user wants to be authenticated by the Avaya system. ASG uses Advanced Encryption Standard (128-bit AES key) technology.

Avaya Services accounts use the ASG process to log in to customer-created administrator logins. ASG replaces static password authentication and adds a level of security to system administration and maintenance ports and logins on any Avaya product. Customers can also use ASG if it is enabled in the system license.

A regular password account uses a fixed user name and a password that can be used multiple times to log in to the system. A person or device that can supervise the login messages, such as network sniffers, can capture this password and gain unauthorized access to Avaya products. ASG instead uses a one-time challenge/response mechanism to authenticate users. The user can log in only when the user enters the correct response. The password or challenge is unique for every session and the challenge cannot be reused. Customers can enable ASG from the System Management Interface if the feature is enabled in the system license.

ASG Guard and ASG Guard Plus

The ASG Guard is a device that provides secure access to Avaya products that do not have ASG software as a native application. ASG Guard 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 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, ASG Guard II can also protect administrative access points on up to 16 IP-enabled devices. Therefore, in a VoIP environment, administrator-level users can access only the devices that they have access to.

Comparison of ASG Guard and ASG Guard II

The table on page 86 lists and compares the features of ASG Guard and ASG Guard II.

Table 23: 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
Telephone line consolidation	Y	Y
Collaborative sessions	Y	Y

ASG security products

Other ASG security products that provide additional security options are also available. For more information regarding the Access Security Gateway family of security products, you can log on to http://support.avaya.com/css/Products/P1019.

Toll fraud prevention

Limitation of long distance access

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

- **Tools that restrict unauthorized outgoing calls** discusses several ways to prevent toll-fraud:
    - Class of Restriction (COR) administration
    - Facility restrictions
    - AAR/ARS analysis
    - Restrictions on station permissions, central office, and incoming tie trunks
- **Security measures** suggests 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/permitting calls to specified area codes/numbers
    - Assigning Class of Restriction (COR)
    - Trunk access and transfer restrictions
- **Detecting toll fraud** 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

Configuration of logs and events

Configuration of 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 or through SNMP or both.

All syslog files are stored in the

```
/var/log
folder
.
```

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

Security-related events

Security events are related to the following actions or activities:

- Successful and unsuccessful attempts of log in or log off.
- 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 a user profile
- Any administrative access to local user accounts (view, add, change, delete)
- 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, such as logging configuration, the PAM configuration, or the firewall configuration.

Note:

You cannot disable logging of security events.

The table on page 89 shows the syslog priority and facility for security and non-security events.

Table 24: 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:

- Configuration of SNMP in Communication Manager on page 89
- Configuration of syslog server in Communication Manager on page 91
- Access system logs through the Web on page 95 provides another way to select, filter and view the syslog through the Communication Manager System Management Interface.
- Define permissions to access system logs on page 129 has information on how to assign or restrict user access privileges to the syslog.

Configuration of SNMP in Communication Manager

About this task

The SNMP protocol provides a simple set of operations that permits 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): The SNMP v1 and SNMP v2c are based on plain-text strings known as communities which are passwords that provide any SNMP-based application to gain access to any type of device management information.
- SNMP Version 3 (SNMP v3): This provides secure authentication and communication between managed entities.

To configure SNMP through Communication Manager System Management Interface:

Procedure

1. Go to Agent Status page.
2. Disable the SNMP agent at the Communication Manager System Management Interface (**Alarms > Agent Status** on the left-side navigation pane.
3. Go to **SNMP Agents** page

4. Go to **Alarms > SNMP Agents** on the left-side navigation pane to configure the SNMP agent.

   Note:

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

   On the **SNMP Agents** screen, you can:

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

5. Go to **SNMP Traps** page.

   On the **SNMP Traps** page, you can specify which alarms can be set as traps.

6. Click **Add/Change** to administer alarm traps and their destinations from the **SNMP Traps (Add Trap Destination)** page.

7. To administer alarm traps and the destination of the alarm traps, on the **SNMP Traps** Page, click Add/Change.

Result

The highest SNMP protocol, version 3, is the most secure and permits 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.

Communication Manager security event notifications through SNMP

The document SNMP Reference Guide for Avaya Communication Manager, 03-602013, describes the types of security-related trap notifications that SNMP can deliver to a trap receiver 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 the following Communication Manager activities:

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

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

- *Administration for the Avaya G250 and Avaya G350 Branch Gateways, 03-300436*
- *Administering Avaya G430 Branch Gateway*, 03-603228
- *Administering Avaya G450 Branch Gateway*, 03-602055

Configuration of 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 must send parts or all of the log information to an external server in real time for a variety of reasons.

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

Topics in this section include:

- General syslog guidelines on page 91 details what syslog contains, file synchronization options, and firewall activity for the syslog server.
- Administration of syslog server in Communication Manager on page 92 helps you configure the Communication Manager syslog server.
- Administration of logging levels in Communication Manager on page 93 contains instructions o prevent logging entries for each event, how to filter or select the information that is delivered to the syslog.

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.
- 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 Survivable Core or Survivable Remote 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 syslog server in Communication Manager

About this task

Note:

By default, Communication Manager disables logging to an external syslog server.

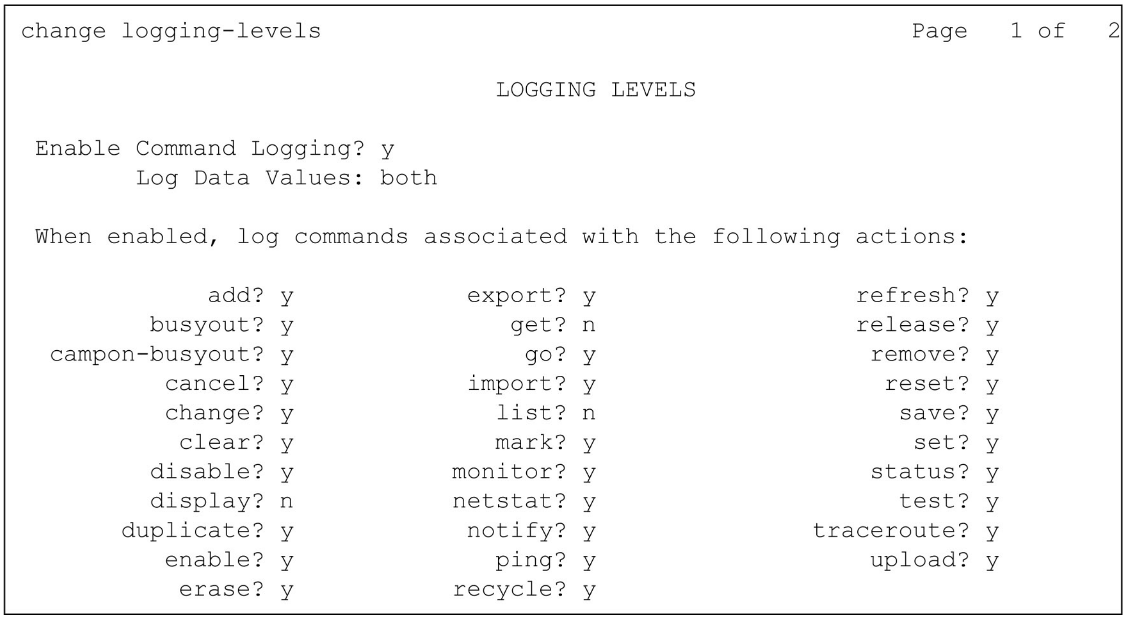
Procedure

1. Log in to Communication Manager System Manager Interface.
2. On the **Administration** menu, click **Server (Maintenance)**.
3. In the left navigation pane, click **Security** > **Syslog**.

   The system displays the **Syslog Server** page.
4. Select the **Control File Synchronization of Syslog Configuration** check box to synchronize the syslog configuration file with a standby or Survivable Core or Survivable Remote Server:
   - To synchronize the syslog configuration of the main server to the standby server, select the **Synchronize syslog configuration to the standby server (duplicated servers)** check box.
   - To synchronize the syslog configuration of the main server to any administered Survivable Core or Survivable Remote servers, select the Synchronize syslog configuration to all **Survivable Core and Survivable Remote servers** check box.
5. Select the **Select Which Logs Are to be Sent to the Above Server** check box to send the following logs to the external syslog server:
   - Security log (/`var/log/secure`)
   - Command history log (/`var/log/ecs/commandhistory`)
   - Communication Manager IP events log (`/var/log/messages`)
   - kernel, boot, cron, `*.`*`info`*, `*.`*`emerg`* logs (`/var/log/messages`)

Administration of logging levels in Communication Manager

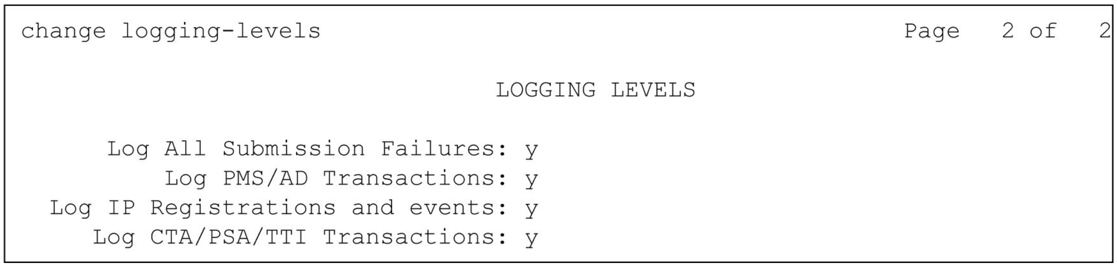
In the **Logging Levels** screen, you can select the activities to supervise in Communication Manager. The figure on page 93 shows an example of the **Logging Levels** screen.



```
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
```

Figure 7: Logging Levels form, page 1 of 2

On the second page of the Logging Levels screen, as shown in the figure on page 93, you can further the information that is delivered to the syslog.



```
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
```

Figure 8: Logging Levels form, page 2 of 2

Logging Level field descriptions

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

Name	Description
	(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.

Access system logs through the web

On Communication Manager System Management Interface, go to the System Logs screen. Some logs listed on the screen are part of the Linux syslog, while the other logs are from Communication Manager

With the **System Logs** screen, you can:

- 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.

For more information, see Define permissions to gain access to system logs on page 129.

Chapter 4: Network Security Integration

Firewall and topology configurations

Firewall settings in Communication Manager

You can administer Communication Manager firewall settings on the Firewall section of the Maintenance Web Page, which is a front-end to the standard Linux command **`iptables`**. IP Tables are used to set up, maintain, and inspect the IP firewall rules in the Linux kernel. These rules can be divided into the following categories:

- The IP input chain
- The IP output chain
- The IP forwarding chain
- The user-defined chains

In the Maintenance page, you can administer the input chain only. The output chain and forwarding chain are set to **accept**. There is no user-defined chain.

⚠ **Warning:**

By default, the IP services that are checked on the Firewall page are already enabled. To disable IP services, you must manually deselect the services. While disabling common IP services, you must ensure that the common IP services do not adversely affect the Avaya server.

Communication Manager firewall default settings

The table on page 97 lists the Communication Manager firewall default settings:

Table 25: Default Communication Manager firewall settings

Input to server	Output from server	Service	Port/protocol
X	X	ftp	21/tcp

Input to server	Output from server	Service	Port/protocol
X	X	ssh	22/tcp
X	X	telnet	23/tcp
	X	domain	53/udp
		bootps	67/udp
		bootpc	68/udp
		tftp	69/udp
X	X	http	80/tcp
X	X	ntp	123/udp
X	X	snmp	161/udp
X	X	snmptrap	162/udp
X	X	https	443/tcp
	X	syslog	514/udp
		ldap	389/tcp
		ldaps	636/tcp
		radius	1812/udp
		securID	5500/udp
		safeword	5030/tcp
		http-ipphone	81/tcp
		https-ipphone	411/tcp
X		hp-sshd	2222/tcp
X	X	secure-sat	5022/tcp
X	X	def-sat	5023/tcp
X	X	echo-request	8/icmp
		ipsi-cmds	1956/tcp
		pcd-ipsi	5010/tcp
		ipsivsn	5011/tcp
		ipsilic	5012/tcp
		licsvr	5423/tcp
X	X	ewl	5424/tcp
		filesync-old	21873/tcp

Input to server	Output from server	Service	Port/protocol
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

Best practices for networking

Separation of network functionality

The following sections explain the benefits of separating the network path of bearer data and control data.

Control and bearer signaling separation

Communication Manager networks always have a control network and a bearer network. The control network carries call processing signals from the endpoints, to the gateways that connect endpoints, and the server or servers. The bearer network carries the voice signals between endpoints. In some cases, the control and bearer networks are carried over the same routes.

In the case of a Duplicated Server that connects to the 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 Processor circuit pack in the Gateway and connects the endpoints over the LAN.

The routes that control signals take between endpoints and the server can be different from the routes that bearer signals take. For example, when you enable the Inter-Gateway Alternate Routing (IGAR) feature, control signals can continue to pass over the normal network of Ethernet switches, routers, C-LAN circuit packs, and IPSIs, and the bearer signals can 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 personal computer of the user, and the bearer signaling is routed over the PSTN to the telephone of the user.

Control and bearer signaling in VLANs

For enhanced security, you can assign different VLANs to the control network and bearer network. At some or all points in the communication path, the devices in the control network and bearer network can 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. Therefore, you must assign the IP telephone and Ethernet port to both the control network and bearer network VLANs. Similarly, when using Processor Ethernet for gateway connections on the Communication Manager Server, you must assign the server to both the VLANs.

However, you can assign Ethernet switch and router ports to a single VLAN to provide separate routes between endpoints. In this way, the separation of VLANs enhances the security on both network segments.

Layer 2 and Layer 3 hardening

To ensure the Communication Manager system is secure, the customer must secure devices in the communication system network at Layer 2, the data link layer, and Layer 3, the network layer, as defined by the Open Systems Interconnect (OSI) 7-layer network model. Communication Manager offers logging capabilities, which the customer can use to detect actual and potential security breaches. For further information, see section Configuration of SNMP and syslog on page 88. To detect security breaches at Layers 2 and 3, customers can also install additional host intrusion and network intrusion detection systems to the network.

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 Branch Gateways, G430/G450 Branch gateways, the IG550 Integrated Gateway, and third-party Ethernet switches and routers that provide LAN/WAN connectivity. If the Communication Manager server is an S8300D Server embedded in a G250-series, G350 Branch Gateways or

G430/G450 Branch Gateways, the router capabilities of these gateways can protect data flowing to Communication Manager without the need for a separate router.

The security features you can use are as follows:

- Generic Routing Encapsulation tunneling on page 101
- IP Security virtual private network on page 101
- Access control lists on page 103
- 802.1X and LLDP on page 109

Note:

G450 and G430 Branch gateways do not support 802.1X and LLDP features.

Generic Routing Encapsulation tunneling

Generic Routing Encapsulation (GRE) is a multi-carrier protocol that encapsulates packets with an IP header and enables the packets to pass through the Internet through a GRE tunnel. A GRE tunnel is a virtual interface between two routers. The first router encapsulates the packet and sends the packet 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 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 Branch Gateway, see *Administration for the Avaya G250 and Avaya G350 Branch Gateway*s, 03-300436.

For more information on administering GRE tunneling on G430 Branch Gateway, see *Administering Avaya G430 Branch Gateway*, 03-603228.

For more information on administering GRE tunneling on G450 Branch Gateway, see *Administering Avaya G450 Branch Gateway*, 03-602055.

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.

IP Security virtual private network

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. Using IPSec with tunneling creates a virtual private network (VPN). On the G250-series and G350 Branch Gateways, IPSec support can be administered for optimal Quality of Service.

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

The G250-series and G350 Branch 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 key.
- 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.
- Security policy with bypass capability for every interface.
- Smooth integration with the on board 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 and GRE.
- 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 an IP address.
- Remote peer failover support.
- Standard and legacy methods of NAT traversal support.
- 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 a Duplicated-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 branch 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 Branch Gateway, see *Application Note: G350 and G250 R3.0 IPSec VPN*, which is available on the Avaya support website at http://support.avaya.com/.

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

Access control lists

You can use Access Control Lists (ACLs) on the Avaya G250, G350, G430, G450 Branch Gateways, or the IG550 Integrated Gateway. Use ACLs to determine which applications, networks, and users can gain access to the hosts on your network. You can also restrict internal users from accessing specific sites or applications outside the network. Access control lists are based on:

- Permitted values or groups of IP addresses
- Protocols
- Ports
- IP fragments
- DSCP values

Figure 14: Network Security using ACLs on page 104 illustrates how to use access control lists to control traffic on your network.

Note:

G700 Branch Gateway does not provide ACL capabilities or DoS protection. A separate customer-provided router must provide these capabilities.

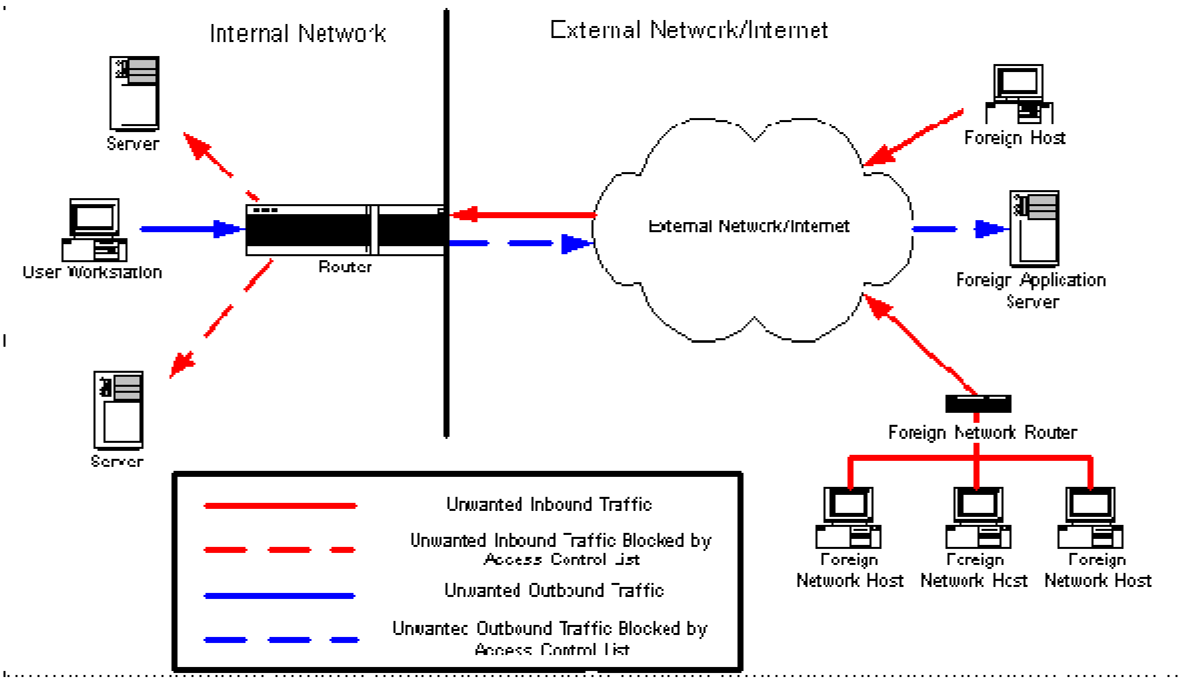

Internal Network
External Network/Internet
Server
User Workstation
Router
Server
External Network/Internet
Foreign Host
Foreign Application Server
Foreign Network Router
Foreign Network Host
Foreign Network Host
Foreign Network Host
Unwanted Inbound Traffic
Unwanted Inbound Traffic Blocked by Access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

Figure 9: Network Security using ACLs

Rules for access control lists

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

- Accepts the packet or drops the packet.
- Sends an ICMP error reply if the gateway drops the packet.
- Sends an SNMP trap if the gateway drops the packet.

For more information, see:

- *Administration for the Avaya G250 and Avaya G350 Branch Gateway*s, 03-300436
- *Administering Avaya G430 Branch Gateway*, 03-603228
- *Administering Avaya G450 Branch Gateway*, 03-602055

External authentication of server administrator accounts

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

AAA Services permit the following 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

External authentication account server requirements

External authentication account server requirements are listed in the table on page 105.

Table 26: External Authentication Accounts

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

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 does not support any other external identity management systems.

For detailed information on configuring external AAA Servers, see *Avaya Aura® Communication Manager Administrator Logins* on the Avaya Support website at http://support.avaya.com/.

LDAP servers

The figure on page 106 shows the tested configuration for external LDAP servers with Name Service Switch (NSS) and Name Service Caching Daemon (NSCD). Login requires an entry in LDAP only.

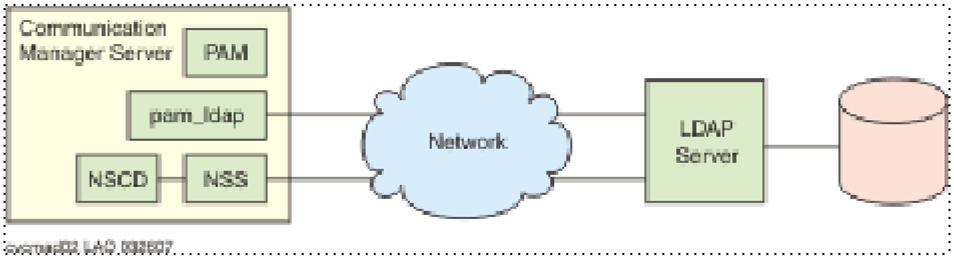


Figure 10: LDAP server authentication configuration

RADIUS servers

An external RADIUS server provides only user authentication and accounting as shown in the figure on page 107.

Note:

Communication Manager Branch Gateways support only RADIUS servers.

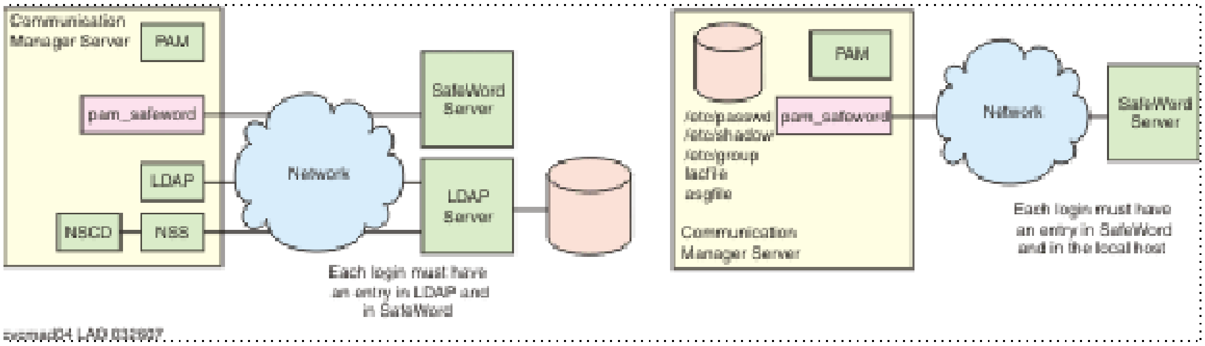

Communication Manager Server
PAM
pam_safeword
LDAP
NSCD
NSS
Network
SafeWord Server
LDAP Server
Each login must have an entry in LDAP and in SafeWord
/etc/passwd
/etc/shadow
/etc/group
lacfile
asgfile
Communication Manager Server
PAM
pam_safeword
Network
SafeWord Server
Each login must have an entry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

Figure 11: RADIUS server authentication configurations

Token servers

RSA SecurID is a token-based authentication method from RSA Security that provides only user authentication. The figure on page 107 shows configurations with an LDAP server and with a local host.

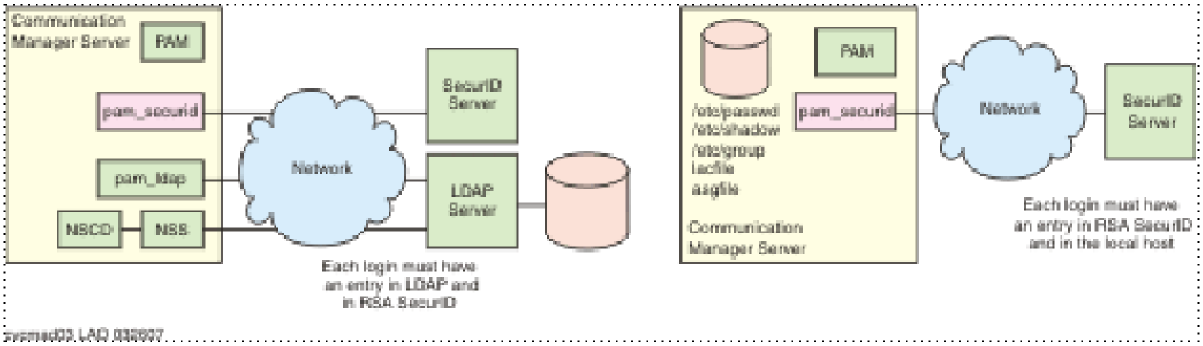

Communication Manager Server
PAM
pam_securid
pam_ldap
NSCD
NSS
Network
SecurID Server
LDAP Server
Each login must have an entry in LDAP and in RSA SecurID
/etc/passwd
/etc/shadow
/etc/group
lacfile
asgfile
Communication Manager Server
PAM
pam_securid
Network
SecurID Server
Each login must have an entry in RSA SecurID and in the local host
cycmad03 LAO 032607

Figure 12: RSA SecurID server authentication configurations

Secure Computing SafeWord is a token-based authentication method from RSA Security that provides only user authentication. The figure on page 107 shows configurations with an LDAP server and with a local host.

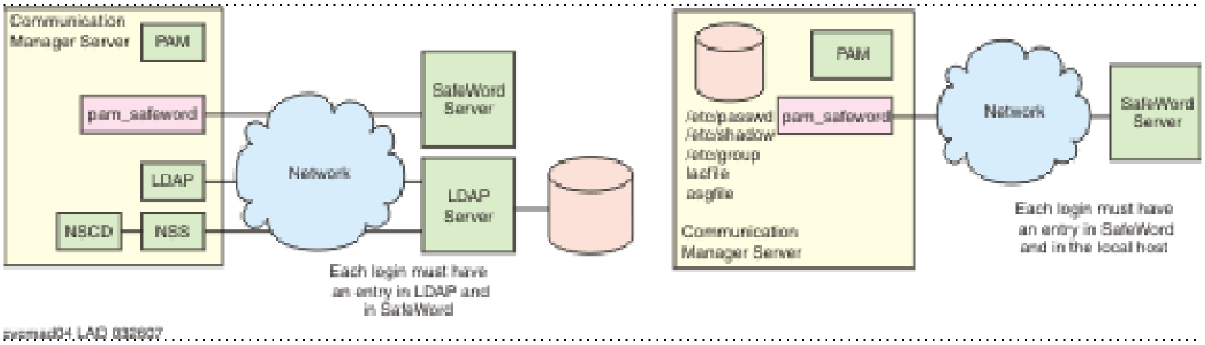

Communication Manager Server
PAM
pam_safeword
LDAP
NSCD
NSS
Network
SafeWord Server
LDAP Server
Each login must have an entry in LDAP and in SafeWord
/etc/passwd
/etc/shadow
/etc/group
lacfile
asgfile
Communication Manager Server
PAM
pam_safeword
Network
SafeWord Server
Each login must have an entry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

Figure 13: SafeWord server authentication configurations

RADIUS plus token servers

The figure on page 108 shows an example of another authentication configuration: RSA SecurID and SafeWord used behind an external RADIUS server.

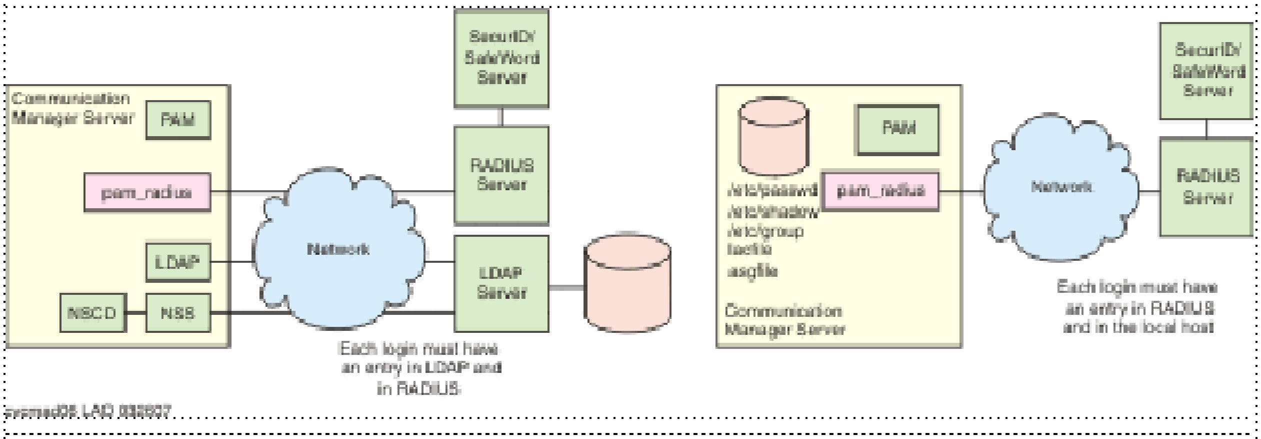


Figure 14: Radius plus token authentication configurations

Administration of external authentication

The Communication Manager default configuration does not contain an entry for an external AAA server. The system authenticates all accounts on the local host.

Customers, not Avaya Services, activate external AAA services. To activate use of an external AAA server, the customer must edit the `/etc/pam.d/mv-auth` file to incorporate the appropriate lines that correspond to the newly added AAA server. The customer must also edit other additional configuration files corresponding to the needs of the AAA service. Customer provides and owns the AAA server on their network and the customers alone have the information necessary to set up clients on the Communication Manager servers.

Additional information on AAA servers

For information regarding configuring external AAA servers, see:

- *Avaya Aura® Communication Manager Administrator Logins* on the Avaya Support website at http://support.avaya.com.
- The website http://www.kernel.org/pub/linux/libs/pam contains PAM documentation such as the System Administrators' Guide.

802.1X and LLDP

The 802.1x protocol authenticates devices at Layer 2. LLDP is a protocol that enables devices to identify themselves to other devices in the network. The combination of the 802.1x and the LLDP protocol prevents unauthorized access to ports and devices at Layer 2.

Separate VLAN groups for functional network segmentation

The Communication Manager network and data networks must be logically separated using virtual LANs (VLANs). You can set up VLANs to isolate devices in the network from other devices. You can also configure VLANs to permit communication between devices across different VLANs using a specifically-designated protocol.

An efficient network separation requires that you establish several different protected VLANs. First, all network devices not specifically used to support telephony must be placed on data VLANs. Data VLANs support Personal Computers, file servers, email servers, and domain controllers. Communication Manager network devices must be placed on different VLANs depending on the role of the devices in the network. VLANs that have similar devices and protocols makes the development, implementation, and management of security features much easier. The following setup is an example of network separation:

- All standalone IP telephones must be placed in their own IP telephone VLANs.
- A Communication Manager sever, which is an H.323 server, must be on an H.323-only VLAN. The Communication Manager server itself must be placed in a different VLAN, depending on the VoIP protocol the customer implements.
- A SIP server, if any, must be placed on a SIP VLAN.
- Softphones must also be placed on separate dedicated VLANs.
- The telephony and data VLANs must have separate servers for standard network services such as DNS, DHCP, and NTP. This is necessary because traffic from these services must not intervene between the telephony network and data VLANs

Customer must also implement switch port level security to prevent an attacker who has physical access to the network from bypassing any VLAN separation by unplugging the network cable of a device and plugging the device of the attacker. The customer must implement 802.1x authentication on IP telephones, Ethernet switches, G250 or G350 Branch Gateways, or IG550 Integrated Gateways.

The Communication Manager server VLAN must 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 telephones, IP interfaces to the IP telephones, the access controller gateway, and the connecting gateway. The gateway VLAN usually contains gateways to an external network such as the PSTN. However, since the gateways usually connect to 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 filters and firewalls

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 gateway VLANs using signaling protocols to authorize and set up calls. The IP telephone VLANs must exchange traffic with the gateway VLANs and with the server VLAN if voicemail applications run on the servers. The Communication Manager Server and telephone VLANs also share administrative protocols so that the Communication Manager Server can configure IP telephones. These might be different protocols than those used by the administrative VLAN. The Communication Manager Server VLAN can provide network services, such as NTP, which can 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 routers or switches must be configured to only permit IP telephones to connect to the Communication Manager Server. In many cases, this means that only VoIP signaling protocols must be permitted between telephones and the Communication Manager server. Filtering must 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 Layer 3 and Layer 4 traffic filtering configured to permit only the protocols required for IP telephony features.

The customer must minimize the traffic between the Communication Manager Server and the data network. For example, the customer must permit users to manage the telephone on a central server that would securely update the IP telephone. To further manage traffic between the Communication Manager VLANs and the data VLANs, the customer can use the Communication Manager Firewall to eliminate unnecessary traffic between the Communication Manager network VLANs and the data VLANs. However, customers can also use router firewalls to provide extensive firewall protection between VLANs.

VLANs in Communication Manager

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

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

The customer can assign the ports on the G250-series, G350, G430, G450 Branch 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 gateway.

The customer can also assign a VLAN to the S8300D server that might be installed in the gateway.

ARP spoofing

A server, gateway, or IP telephone needs the media access control (MAC) address of the target device for communication. Similarly, any device that tries to communicate with an Avaya server, gateway, or IP telephone needs the MAC address of the server, gateway, or IP telephone. When the MAC address is not yet known, the system sends an Address Resolution Protocol (ARP) request along with the IP address of the target device to determine the MAC address of the device. 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 along with the MAC address of device B. Device A then updates the ARP cache to save the MAC address of for any future communications with device B.

An attacker uses an ARP spoofing tool to identify the IP and MAC addresses of the target device. The target device can be a server, a gateway, or an IP telephone. Since the initiating device sends an ARP request as a broadcast, the ARP-spoofing tool can listen for these requests. After determining the IP addresses of device A and device B, the tool 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 instead of the MAC address of device B, and device B has the MAC address of the attacker instead of the MAC address of device A. Therefore, any traffic that comes in or goes out of device A or B, the traffic will always be routed through the attacker computer. With sniffing tools, the attacker can then eavesdrop on calls and sniff the packets for 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

A very good defense against ARP spoofing is to divide the network into separate domains or subnets. ARP spoofing cannot occur when the communicating devices are in different subnets. You can administer gateways and the IP telephones associated with the gateways in separate domains to provide protection against ARP spoofing.

Another possible defense is the use of static ARP entries. Since static entries cannot be updated, the system ignores spoofed ARP replies. To prevent spoofing, the ARP tables must have a static entry for each computer on the network, but the overhead in deploying and updating these tables is not practical for most organizations.

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 network, the need for security of these servers is even greater than the security needs of endpoint 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 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. Therefore, a DHCP server performs IP address pool management.

DHCP vulnerabilities

Each IP telephone automatically sends out a DHCP request for an IP address with which to register. The DHCP server then sends the IP telephone the IP address of the Communication Manager server and any TFTP servers and Survivable Remote servers that are known to the DHCP server. The IP telephone 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 is inherently vulnerable to spoofing as it is not an authenticated protocol. An attacker can provide incorrect network settings to a telephone, 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 denial of service by continuously requesting IP addresses until none are left for legitimate devices.

The attacker can change the firmware of the IP telephone or the configuration file of the IP telephone in the following ways:

- After spoofing the DHCP server, an attacker can perform a man-in-the-middle attack to intercept and replace the files as they are downloaded from the server.
- The attacker can compromise the server that stores the firmware and configuration files of telephones. This is a more serious problem as control of a download server enables the attacker to target all telephones in an organization.

DHCP security

To provide greater security to DHCP servers in a network, you can use one or more of the following security measures:

- Assign static IP addresses to the Communication Manager server and gateways. For more information, see the appropriate installation document for Communication Manager servers.

  You can also assign static IP addresses to IP telephones that serve critical functions. However, this option is often impractical as the IP telephones of an organization are numerous and frequently keep changing. In addition, with a static IP address, each time an IP telephone reboots, the telephone does not automatically re-register with the servers. For more information, see the document *4600 Series IP Telephone LAN Administrator Guide,* 555-233-507.

  As with the Communication Manager server, C-LAN and processor circuit packs are assigned static IP addresses. For more information, 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 telephone deployment and disable DHCP once registration is complete. You can safely enable DHCP when the network is protected by anti-spoofing features that keep associations of IP address, MAC address, and switch port in access and infrastructure devices.

  Loss of LAN connectivity causes IP telephones to search for an IP address, therefore disabling DHCP can be impractical. In the event of a break in LAN connectivity, IP telephones cannot reregister until the DHCP server is enabled again.

- Use separate DHCP servers to support the devices in the IP telephony 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 single geographical location, attacks on a particular DHCP server are limited to physical access points within that particular geographical location.

  Use the Communication Manager IP Interface screen and the Network Mapping screen to assign VLANs to IP telephones and gateways. In addition, use the Locations, Location Parameters, and Network Region screens to further define the characteristics of each VLAN. Finally, administer a DHCP server support for 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 gateways before connecting to the network.
- Administer network switches, when possible, to associate Ethernet address, IP address, and switch ports. When the system receives a packet with an address that does not match on a port, the system drops the packet.
- Encrypt all firmware and configuration files that you download over the network. Ensure that all the telephones have the signature verification key loaded in a secure manner. The telephone must verify the signature on every downloaded file 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.

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 servers, DNS servers are also 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 provide greater security to DNS servers in a network, you can 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 might be unlawful in some countries and could enable an attacker to determine the existence of the DNS clients in the zone.

Communication Manager approach towards 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 suggests methods for reducing those risks. The risks fall under the following categories:

- Confidentiality and privacy on page 114
- Integrity issues on page 117
- Availability and Denial of Service on page 118

Confidentiality and privacy

In a telecommunications switch, eavesdropping on conversations is a serious concern, but the confidentiality of other information on the switch must also be protected against toll fraud, voice and data interception, and denial of service attacks. When compared to TDM systems, VoIP communications system is more vulnerable as eavesdroppers can access the packets in the network surreptitiously.

The following sections describe the vulnerabilities to confidentiality and privacy, each with a NIST recommendation for reducing the vulnerabilities and a description of how Communication Manager addresses the vulnerability.

Switch default password vulnerability

NIST recommendation: You must change the administrative or root passwords frequently to prevent wiretapping of conversations on the network. If possible, you must disable remote access to the graphical user interface to prevent the interception of plaintext administration sessions. When possible, a direct USB connection to the administrative interface is recommended. Also, you can try 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 superuser login must be administered before the installation is 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 a 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 telephones and use an alarm system for notifying the administrator when an IP telephone is disconnected so that the system is closed to this kind of an attack.

How Communication Manager addresses the vulnerability: IP telephones of Avaya have the option of manually disabling the secondary hub. Communication Manager logs events such as the disconnection of an IP telephone. In addition, an alarm is generated when an IP telephone is disconnected. For further information on Communication Manager generated alarms, see *Maintenance Commands for Avaya Servers, and Gateway*s, 03-300430

ARP cache poisoning and ARP floods

An ARP flood attack could render the network vulnerable to 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: The section Security strategies to combat ARP spoofing on page 111 discusses more on how Communication Manager addresses this kind of a vulnerability.

Web server interfaces

When an administrator uses a web server interface for remote or local administration, an attacker with access to the local network can sniff plaintext HTTP packets to gain access to 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 protocol.

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

IP telephone subnet mask vulnerability

An attacker can assign a subnet mask and router address to an IP telephone, which can cause the computer of the attacker to receive all the packets that the IP telephones transmit. This kind of intrusion is 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 permits the customer to turn on or turn off various protocols and ports when not needed. In addition, the G250-series and G350 Branch Gateways and the IG550 Integrated Gateway support access control lists for traffic accessing the Communication Manager network.

Extension to IP address mapping vulnerability

An attacker can determine the IP address of an extension by calling that extension. Once the call is answered, the attacker can use a protocol analyzer or packet capture tool attached to the hub on the dialing instrument to capture packets flowing directly to and from the target instrument. Once the attacker acquires the IP address of a particular extension, the attacker can also accomplish other attacks. If the attacker does not know the IP address of the target telephone, then it is difficult for the attacker to view the packets sent and received by the target telephone.

NIST recommendation: Enable the hub on the IP telephone only when necessary.

How Communication Manager addresses the vulnerability: IP telephones of Avaya have the option of manually disabling the secondary hub. For more information, see section Secure updates of Avaya software and firmware on page 157.

Integrity issues

Integrity of information means that information remains unaltered by unauthorized users. Misuse of information might not necessarily involve illegitimate users. A legitimate user can also perform an incorrect, or unauthorized operation. This is possible because of several factors, including the possibility that the level of access permission granted to the user is higher than what the user needs. Information can be compromised in one of the following ways:

- An intruder acquires the credentials of a legitimate user and accesses an operations port of the switch. Then, the intruder can perform the following operations:
    - Disclosing confidential data
    - Causing service deterioration by modifying the system software
    - Crashing the system
    - Removing all traces of the intrusion by modifying the security log
- There can be situations when the system becomes vulnerable because:
    - After a system restart or during a disaster recovery, the default security features such as passwords are reverted to the default system password.
    - At the time of installation, the switch is vulnerable until the default security features are installed.

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 giving rise to possible “man in the middle” attacks on the gateway and supported IP telephones. With ping flooding and MAC spoofing, an attacker can remotely reboot an IP telephone that starts generating DHCP server requests.

NIST recommendation: If possible, use static IP addresses for the IP telephones. Using static IP addresses 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, permitting 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 112.

TFTP server insertion attack

When an IP telephone is being reset, a rogue TFTP server responds to a TFTP request instead of the legitimate TFTP server. Then, the attacker might reconfigure the target telephone.

NIST recommendation: Use a state-based intrusion detection system to filter out DHCP server packets from IP telephone ports, permitting 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 the IP telephones of Avaya support secure file transfer using the HTTPS protocols. The G250-series and G350, G430, G450, Branch Gateways and the IG550 Integrated Gateway support SCP protocol for configuration files transfer. For more information, see Secure backups of Communication Manager data and translations on page 156.

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 can lead to deterioration or denial of service. A network can become vulnerable to denial of service attacks when the capacity of the network is overloaded. A denial of service attack on VoIP is easily possible because of 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 by providing the maximum number of characters for the login and password buffers multiple times in succession. IP telephones can also 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 include intrusion vulnerabilities.

NIST recommendation: The deployment of a firewall that rejects connection requests 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 permits the customer to turn on or turn off various protocols and ports when not needed. In addition, the G250-series, G350, G430, G450 Branch 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. For more information, see section Security strategies to combat ARP spoofing on page 111.

Account lockout vulnerability

An attacker can provide several incorrect login attempts at the telnet prompt until the account is locked out. The account cannot connect to the device for the set lockout time.

NIST recommendation: If remote access is unavailable, this problem can be solved with physical access control.

Communication Manager workaround: Communication Manager disables Telnet by default. Users must use SSH for remote access. Physical access through a serial console is available on every Communication Manager server.

Recommendations for preventing DoS attacks

To eliminate DoS attacks, organizations can perform the following:

- Mitigate call processing overloads.
- Activate remote managed services.
- Use Signaling groups.

Mitigating call processing overloads

About this task

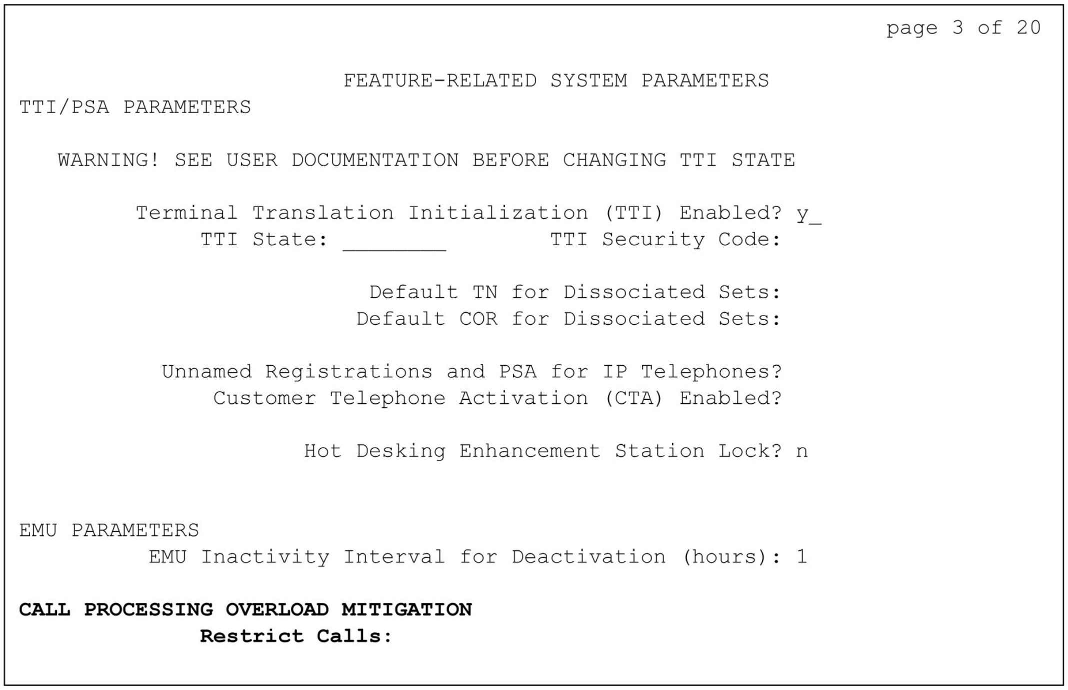
Communication Manager monitors and reacts to call processing overload conditions as a defense against DoS attacks. You can administer Communication Manager to regulate inbound and outbound trunk traffic.

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

Procedure

1. On the SAT screen, type **`change system-parameters features`**.

   The system displays the Feature-Related System Parameters screen.



```
                                                                   page 3 of 20

                         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:

                           Default TN for Dissociated Sets:
                          Default COR for Dissociated Sets:

           Unnamed Registrations and PSA for IP Telephones?
               Customer Telephone Activation (CTA) Enabled?

                      Hot Desking Enhancement Station Lock? n


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

CALL PROCESSING OVERLOAD MITIGATION
              Restrict Calls:
```

Figure 15: Feature-Related System Parameters screen

2. Administer the call processing overload mitigation.

   Field values and descriptions for Restrict Calls explains the different values that you can enter for the **Restrict Calls** field.

Field values and descriptions for Restrict Calls

Name	Description
stations-first	The direction for this restrict call is inbound. Denies new traffic generated by internal stations, permitting inbound calls only (best for call center environments).
all-trunks-first	The direction for this restrict call is outbound. Denies all outbound calls to trunks, tie-lines, and stations, and all station-originated calls.
public-trunks-first	The direction for this restrict call is inbound. Denies all inbound calls from trunks and tie-lines.

Activate 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 Branch Gateway or a C-LAN or MEDPRO that:
  - Detects DoS attacks.
  - Registers goes into service, and de-registers goes out of service or resets.
- IP endpoint or Enterprise Mobility User (EMU) that attempts to register with an invalid PIN or invalid extension
- IP endpoint that registers (goes into service), de-registers (goes out of service), or resets

At the Communication Manager SAT interface, type the **`change system-parameters security`** command to administer Remote Managed Services.

```
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
```

Note:

The default value of the **RMS Feature Enabled** field is **n**, meaning that the Remote Managed Service feature is disabled.

Use the recommendations in which table to alert you of security-related events, including DoS conditions.

Setting Denial of Service attack notifications through Managed Security Services

Procedure

1. Set the **RMS Feature Enabled** field to **y**.

When you set this field to **y**, the **Port Board Security Notification** and **Port Board Security Notification Interval** fields is visible. Default is **n**.

2. Set the **Port Board Security Notification** field to **y**.

   When you enter **y** in this field, the **Port Board Security Notification Interval** field is visible. Default is n.

3. Enter the required interval (in seconds) between port board Denial of Service notifications (traps). The value of the interval is 60 to 3600 in interval of 10. Default is **60** (1 minute).

   ✱ **Note:**

   There is no delay before the first trap is sent. The interval administered in this field applies only to the period *between* traps.

Use Signaling groups

You must specify both ends of a signaling group to secure a connection. Incomplete administration of the connection, that is, not specifying both the near-end and far-end IP addresses permits an attacker to access the signaling group connection and the call setup data. Communication Manager displays a Denial of Service vulnerability warning if you do not administer both ends of the connection.

Use the **`add signaling-group n`** command, where **`n`** is the signaling group number, to create a new signaling group. Use the **`change signaling-group n`** command, where **`n`** is the signaling group number, to edit an existing signaling group. Note that the value of the **Group Type** field on the **Signaling Group** screen must be **h.323** or **sip**.

Signaling Group screen field descriptions

The table on page 122 to prevent DoS vulnerabilities from incomplete SIP or H.323 signaling group administration on the Signaling Group screen.

Table 27: Mitigating Denial of Service attacks through signaling group administration

Signaling group field	Group Type	Fieldvalue	Description
Far-end Domain	**sip**	40-characterstring	This field specifies the IP domain for which the far-end proxy is responsible (that is, authoritative), if it is different from the near-end domain. If the domains are the same, leave this field blank.
		blank	No warning.

Signaling group field	Group Type	Fieldvalue	Description
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.

For more information, see section Description of the Security Violations Status reports on page 134.

Chapter 5: Operational Security

Description of 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 the core products of Avaya.
- 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:

- 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 that vulnerability and assigns one of four risk levels: **High, Medium, Low**, and **None**. For more information on interpreting a security advisory, see section Interpretation of Avaya Security Advisory on page 126. Depending on the category of the risk, the PSST creates an Avaya Security Advisory to notify customers of the vulnerability.

Depending on the vulnerability and the risk level, the advisory can include:

- A recommended mitigation action.
- A recommendation to install a third-party patch.
- A recommendation to install a software patch provided by Avaya.
- A recommendation to upgrade existing software.
- Additional guidance regarding the vulnerability.

Timeframe of 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 subscribed to receive advisories. The advisories are distributed in a timeframe as indicated in the table on page 126:

Table 28: Avaya Security Advisories time frames

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

Subscribing to Avaya Security Advisories

Customers must perform the following steps to receive security advisories from the Avaya Security Support website by email:

1. Log on to http://support.avaya.com.
2. On the bottom of the page, click on **Set E-notifications**.
3. If you do *not* have an account, click on **Registration Now** and follow the instructions to create an account.
4. Log in using your existing credentials.
5. Select **Security Advisories** and click **Submit** to receive notifications of all security advisories.

   To receive notifications on creation or updates of security advisories of a specific product, select a product from the product list and from the release version page, select the product version and click **Continue.**

   The system displays a confirmation page. You are now ready to receive e-mail E-Notifications whenever an Avaya Security Advisory is updated or published.

Interpretation of Avaya Security Advisory

For precise definitions that the Avaya Product Security Support Team (PSST) follows in classifying vulnerabilities relative to their potential threat to Avaya products, see *Avaya's Security Vulnerability Classification*. You can download this document from http://support.avaya.com.

The table on page 127 summarizes the three main categories.

Table 29: Avaya security vulnerability classification

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

Structure of an advisory

Each Avaya Security Advisory contains the following information:

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

  For operating system or third-party software, Avaya provides a link for quick access to a website that provides the following information:

  - A description of the risk
  - Instructions on how to correct the problem. The instructions can include:
    - Installing an update
    - Reviewing administration of the product
  - A description of additional security fixes, if any, are also included in the update.
- **Avaya Software-Only Products:** This section contains a listing of the specific Avaya products that use, but are not bundled with, operating system software that can be vulnerable. The information in this section includes:
  - The version of the affected product
  - Possible actions to take to reduce or eliminate the risk
- **Avaya System Products**: This section contains a listing of the individual Avaya products that are vulnerable or products that are bundled with operating system software that are vulnerable. The information in this section includes:
  - The level of risk
  - The version of the affected product
  - Possible actions to take to reduce or eliminate the risk
- **Recommended Actions**: This section contains steps to take to eliminate the vulnerability. The steps can 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 listed out in detail through the website links in the security advisory.

Integration of security updates in Avaya applications

When a third-party patch is available to mitigate a security vulnerability, Avaya can advise the customer to apply the patch from the third-party. This action is stated explicitly in the Avaya Security Advisory.

Customers might not install some third-party updates due to interoperability, stability, or reliability issues with the update in relation to Communication Manager. In this case, before

Avaya releases a security update, Avaya thoroughly tests the update on a non-production system, along with all the other software that is normally loaded on a Communication Manager server. Sometimes Avaya must modify the update before the update works correctly. Customers who apply third-party patches without Avaya recommendation void the warranty of the Avaya products.

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

Audits and security logs

Removal of old logins

You must remove unused administrator accounts to prevent unauthorized access to sensitive logs and files. With Communication Manager System Management Interface, you can add, change, lock, or remove administrator logins and login groups for the Communication Manager server. Communication Manager System Management Interface does not manage logins that are authenticated in an external server such as LDAP.

You must use the **Security > Administrator Accounts** page, to remove administrator accounts. For further information on removing administrator accounts, see *Avaya Aura® Communication Manager Feature Description and Implementation (555-245-205)*.

Define permissions to access 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 the default permission setting for Profile 18 (superuser) and Profile 19 (user), see *System Management Interface default profiles and permissions*.

For a complete discussion of the Web Access Mask page, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Security information log

Security information is logged in or notified through the following:

- SNMP trap receiver. For more information, see section Configuration of SNMP and syslog on page 88.
- Syslog security log. For more information, see section Configuration of syslog server in Communication Manager on page 91.
- Miscellaneous logs viewed from the Systems Log page track the following 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

Interpretation of the security logs

Description of the syslog header

Each syslog entry has a common header format:

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

Table 30: Syslog entry header format description

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

Syslog header example

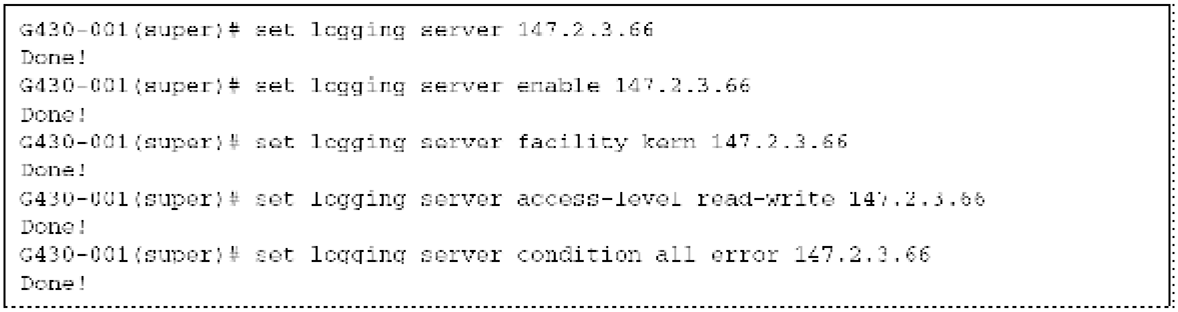
```
20070326:061058000:7103:cmds:MED:
```

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

Syslog server example for a branch gateway

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

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



```
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!
```

Figure 16: Syslog server for G430 gateway

Description of SNMP entries in the syslog

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

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

Table 31: SNMP agent log description

Log entry	Description
module-name	The name of the SNMP module logging the event
pid	The Linux process ID of the process initiating the log entry

Log entry	Description
snmp	The text string “snmp”
ip	The ip address of the management system
R	Result codes: • s: action was successful • f: action failed for non-security reason • v: action failed due to a security violation **Note:** An ASCII error code might follow the letter “f” and an optional colon (:), for example, “f:123456.”
set	The string “set”
object	A human readable name for the object being accessed
value	The new value for the object being set.

SNMP log example

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

Note:

Only sets are logged, gets are not.SNMP agents log a single asterisk (*) for any passwords, pins, encryption keys, or security tokens, if any.

Description of the platform command history log

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

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

Table 32: Platform command history log descriptions

Field	Description
mmm	The month in text format, for example “Aug”
dd	The day of the month
hh:mm:ss	The time in 24-hour format
server-name	The host name of this server

Field	Description
text	The text field contains the log event text that is supplied by the module logging the event. For on the text field see the following sections: • Description of the command history log for SAT on page 135 • Description of the command history log for Web activity on page 137

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**.

Viewing Communication Manager security violations through SAT

Before you begin

Before running the **monitor security-violations** command, ensure that the **RMS Feature Enabled** field on page two of the **Security-Related System Parameters** screen is to **y** before the **monitor security-violations** command will run (see Activate Remote Managed Services on page 121).

About this task

Use this procedure to view Communication Manager security violation through SAT. You can 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

Procedure

On the system access terminal screen, type `monitor security-violations` to see more information about failed attempts to access the system.

Security Violations Status field descriptions

Name	Description
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	Trunk group through which the security violation occurred.
TG No	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.
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	

Description of the Security Violations Status reports

Depending on the command qualifier, the Security Violations Status reports differ slightly.

For field descriptions, see *Security Violations Status field descriptions*.

```
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
```

Description of the command history log for SAT

Depending on the level of logging that you enable, the format for the text portion of log entries for SAT, following the syslog header, is:

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

For a list and description of the text formats in the log entry for SAT, see *Communication Manager SAT command history log format*.

For more information about logging levels, see Administration of logging levels in Communication Manager on page 93.

Communication Manager SAT command history log format

Name	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 numeric ID of the SAT user.
uname	The login name of the SAT user.

Name	Description
uname2	The secondary login name of the SAT user.
profile	The access profile number that is assigned to this user.
R	The status of the action: • **s**: The action successful. • **f**: The action failed due to a non-security related reason. An ASCII error code might follow the letter "f" and an optional colon (:), for example, "f:123456." • **v**: The action failed 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.

SAT log example

Security alert:

The system does not display authorization codes, PINs, encryption keys, and passwords in the command history log.

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

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

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

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

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

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

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

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

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

These entries indicate the following:

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

> **Note:**
>
> For commands that log new entries, the system logs only values that change from a default value.

Description of the command history log for Web activity

Depending on the information on a Web page, the text formats for log entries 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
```

Abbreviated Dialing Button Programming command history log format lists and describes the text formats in the log entry for Web activity.

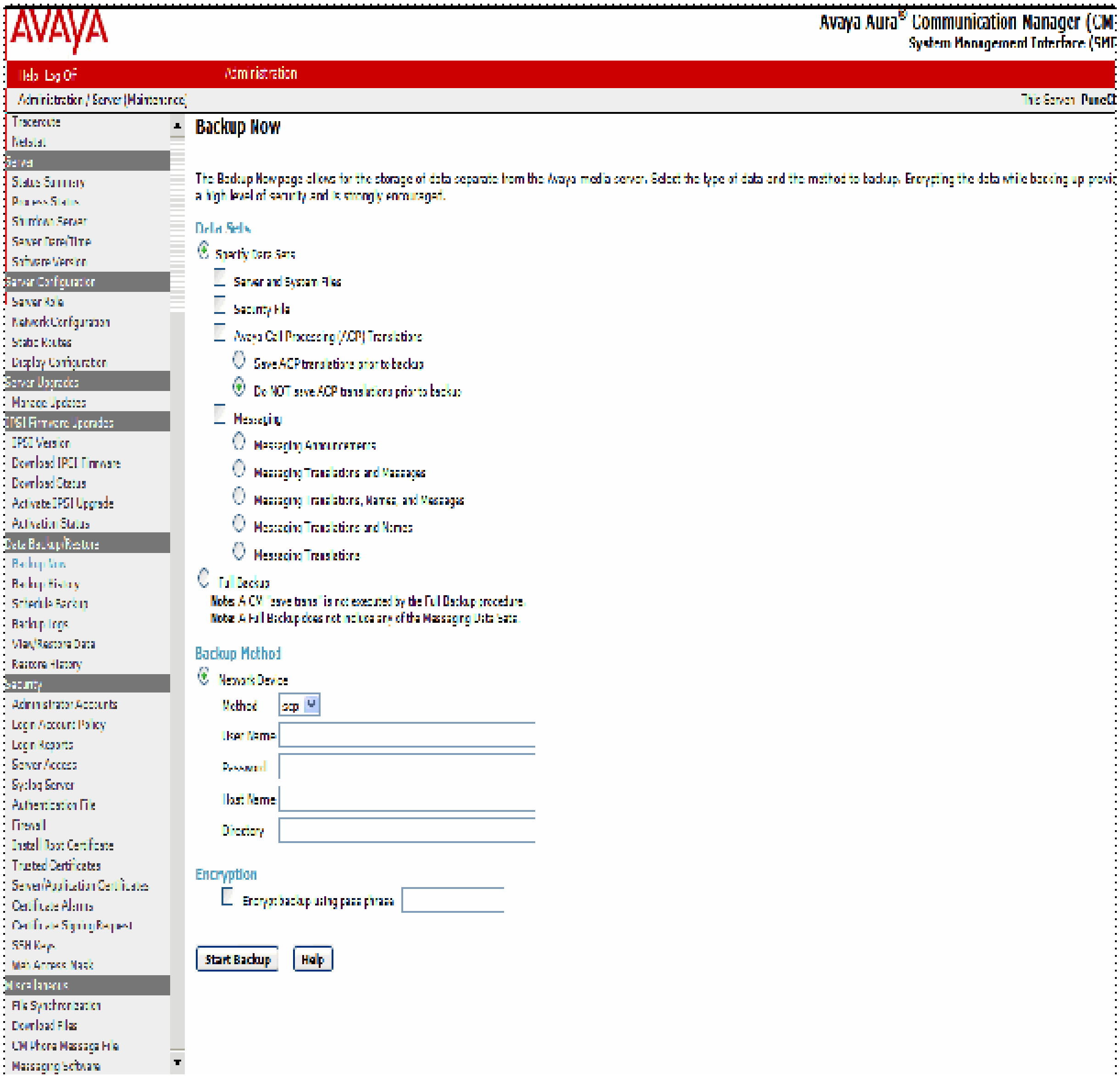
Abbreviated Dialing Button Programming command history log format

Name	Description
module-name	The name of the software module that created the entry in the log

Name	Description
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 of user establishing the web session.
profile	The access profile number assigned to the user
R	The status of the action: • **s**: The action is successful. • **f**: A nonsecurity-related reason is causing the action to fail. An ASCII error code might follow the letter f and an optional colon (:), for example, f:12345 • **v**: A security violation is causing the action to fail.
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.
variable-name	The name of the text box, button, or check box.
value	The value of the variable name after the change. When the variable name is the name of a check box, the value is checked or unchecked.

Web log entry example

For example, consider the **Backup Now** page shown in the figure on page 139 (the page as it is initially presented to the user).



Backup Now

The Backup Now page allows for the storage of data separate from the Avaya media server. Select the type of data and the method to backup. Encrypting the data while backing up provic
a high level of security and is strongly encouraged.

Data Sets

● Specify Data Sets

□ Server and System Files

□ Security File

□ Avaya Call Processing (ACP) Translations

○ Save ACP translations prior to backup

● Do NOT save ACP translations prior to backup

□ Messaging

○ Messaging Announcements

○ Messaging Translations and Messages

○ Messaging Translations, Names, and Messages

○ Messaging Translations and Names

○ Messaging Translations

○ Full Backup

Note: A CM "save trans" is not executed by the Full Backup procedure.
Note: A Full Backup does not include any of the Messaging Data Sets.

Backup Method

● Network Device

Method scp

User Name

Password

Host Name

Directory

Encryption

□ Encrypt backup using pass phrase

Figure 17: Backup Now page with initial defaults

The user must then perform the following changes:

- Uncheck the box labeled **Avaya Call Processing (ACP) Translations**.
- Check the box labeled **Security Files**.
- Select SCP and enters appropriate data.

The log entries created following the syslog header are similar to the following:

```
some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now
```

```
some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now | acp xln
| uncheck
```

```
some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now | security
files | check

some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now | ftp |
check

some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now | user
name | backupoperator

some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now | password
| *

some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now | hostname
| dataserver

some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now |
directory | /cm

some-web-module[123456]: web 192.11.13.5 778 login 0 s backup now | button
| start backup
```

Only the first event is logged unless the user clicked the **Start Backup** button. Field changes are not logged unless the page is actually submitted. The field name **Avaya Call Processing (ACP) Translations** is abbreviated to try to make the log entry short but recognizable.

Software and firmware updates

Classification of security updates

Avaya makes security updates available on or through the Avaya Security website 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 provides remediation actions based on the following target intervals:

Table 33: Vulnerability classifications and remediation intervals

Vulnerability	Target remediation intervals
High	If Avaya needs to develop a software update, the Avaya Security Advisory provides a timeline for availability of the update. Avaya incorporates the fix into a separate service pack or update. The maximum delivery time for the service pack or update is 30 days.

Vulnerability	Target remediation intervals
	If a software patch is available for installation or another action is recommended, the Avaya Security Advisory describes the actions.
Medium	If Avaya needs to develop a software update, Avaya includes the update in the next major release that can 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. The maximum delivery time for the service pack or update is 1 year. If a software patch is available for installation or another action is recommended, the Avaya Security Advisory describes the actions.
Low	If Avaya needs to develop a software update, Avaya includes the update in the next major release that can reasonably incorporate the update. If no new major releases are scheduled for a product, and Avaya is providing maintenance support, Avaya incorporates the fix into a separate service pack or update. The maximum delivery time for the service pack or update is 1 year. If a software patch is available for installation or another action is recommended, the Avaya Security Advisory describes the actions.
None	No remediation actions are required.

Avaya incorporates a third-party update into Avaya software in one of the following ways:

- Avaya 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 Avaya product software, the fixes can be delivered in one of the following ways:

- A security update: A security update includes operating system security fixes or third-party software security fixes or both.
- 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.

Validation of a security update

When Avaya determines that a third-party security update applies to one or more of Avaya products, the product development team tests the update on the affected products to ensure there are no adverse affects to the published functionality of the products. In addition, Avaya thoroughly tests the third-party updates that are included in new software releases.

Avaya-generated security updates are also 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

Security updates for the operating system

Operating system security updates for Communication Manager servers are usually applied separately from other platform or Communication Manager software updates. If Avaya issues a security update, the customer can apply the update themselves or engage the service support group to apply the update.

Instructions for applying a security update are normally provided either in the security advisory or as instructions on the website for updates of the associated operating system or application package. For more information, log on to http://support.avaya.com/security.

For Communication Manager, the **Manage Updates** Web pages facilitate applying the security updates.

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 can result in creation of a Communication Manager software update.

If Avaya issues an Avaya software update, the customer can apply the update themselves or engage the service support group to apply the update. In most cases, the customer is responsible for applying the update unless the Maintenance contract of the customer 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 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.

Security updates and advisories

For each security update for a third-party application or the operating system, the referencing security advisory provides a link for quick access to the third-party website. Such websites 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 an FTP site that stores the update and a readme file that describes the security fixes in the update.

Avaya can bundle 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 customer installs the package, the customer can use Communication Manager Manage Software Web page to locate the file containing the security update.

Determining the contents of a security update

About this task

The following steps help determine the contents of the file containing the security update:

Procedure

1. Log on to the Avaya support Web page at http://support.avaya.com.
2. Select **Downloads and Documents**.
3. Select **Avaya Aura® Communication Manager**.
4. Select the release number.
5. Select **Latest TN Circuit Pack, Server, and Gateway Firmware and Software Updates**.

   The system displays a Web page containing links Communication Manager-related products.
6. Click on the appropriate firmware release number of the appropriate product.

   The system displays a Web page containing details of the firmware release.
7. View the readme file for the security update package.

Result

On the Linux command line, type the command **`update_info <security patch name>`**, where **`<security patch name>`** is the name of the Avaya security update, to display information about Avaya security updates. The customer can log on to 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

Note:

This law applies to U.S. customers only. Customers must seek appropriate legal advice for interpretation of the requirements of this act. 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. According to this act, public companies must evaluate and disclose the efficiency of the internal controls of 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 security-related features can further demonstrate the good faith of the organization in data management and reporting.

Communication Manager security features also help prevent unauthorized access to the customer network.

For more information about features related to data security, see the table on page 144.

Table 34: Data security features in this guide

Feature	How related to Sarbanes-Oxley	Where documented
Encryption	Transmitted data is protected from packet-sniffing and eavesdropping	See: • Encryption overview on page 37
Access control	Access to data is protected from unauthorized personnel	See: • Access profiles on page 31 • Managing Communication Manager accounts on page 83

Feature	How related to Sarbanes-Oxley	Where documented
Authentication	Access to the system is restricted by login/password.	See: • Access profiles on page 31 • Managing Communication Manager accounts on page 83
Logging	Security-related events are logged	See: • Configuration of SNMP and syslog on page 88
Backup of data	Data saved on backup or backup server. Protected by encryption and key.	See: • Secure backups of Communication Manager data and translations on page 156

Application of Communication Manager data for financial reasons

Communication Manager can generate call detail records that can be used in financial data:

- Communication Manager generates call detail records in real-time and sends the records to the printer or a reporting system that converts call record data into a financial report. Two such reporting systems, eCAS Call Accounting System and VeraSmart Application Suite, are available through Avaya DeveloperConnect partner Veramark Technologies, Inc. These reporting systems provide their own data security. For more information, see http://www.veramark.com.
- Communication Manager transmits Call Detail Recording (CDR) records to call accounting devices over a TCP/IP connection using Reliable Session Protocol, the proprietary protocol of Avaya. The data are protected from corruption, but not encrypted. To safeguard the CDR data, the customer must connect the CDR device directly to the Communication Manager server to export the CDR data.
- The customer can add the following financial data elements in the CDR records:
    - Account codes: Account codes are codes that users manually enter to 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): This is applicable for ISDN trunks. AOC contains information that Communication Manager collects from the public network for each outgoing call. Charge advice is a number representing the cost of a call and can be recorded as a currency unit.
    - Periodic Pulse Metering (PPM): This is applicable for non-ISDN trunks. PPM is data that Communication Manager collects 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 helps in calculating the call 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 can be used to generate financial reports. Similar to the CDR reporting devices, the CMS and Interactive Response systems have a number of security features that can be used to protect data.

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 *Avaya Interactive Response Security.*

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 must seek appropriate legal advice for interpretation of the requirements of this act. 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 methods an institution can use to disclose private information.

According to the policy, financial institutions must protect the critical as well as nonpublic, but personal information of their customers. To ensure this protection, the Graham-Leach-Bliley Act mandates that all institutions establish appropriate administrative, technical, and physical safeguards.

The Graham-Leach-Bliley Act can also apply to Communication Manager data that includes customer names and telephone numbers, called and calling number data, and abbreviated dial lists.

With the following features, organizations can protect customer privacy and demonstrate that the organization is compliant with the interagency guidelines supporting the Graham-Leach-Bliley Act.

Table 35: Communication Manager security and compliance of Graham-Leach-Bliley Act

Feature	Relation to the Graham-Leach Bliley Act	Where documented
Encryption	Transmitted and stored data is protected from unauthorized individuals.	• Encryption overview on page 37
System access control	Access to data is protected from unauthorized personnel.	• Access profiles on page 31 • Managing Communication Manager accounts on page 83
Authentication	Access to the system is restricted by login/password.	• Access profiles on page 31 • Managing Communication Manager accounts on page 83
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	• Secure backups of Communication Manager data and translations on page 156

Considerations for customers who must comply with HIPAA

Note:

This law applies to U.S. customers only. Customers must seek appropriate legal advice for interpretation of the requirements of this act. 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 healthcare providers to disclose to healthcare recipients the ways in which the institution can use and disclose private information. HIPAA also requires healthcare providers to protect the privacy of certain individually identifiable health data for healthcare recipients.

HIPAA can apply to Communication Manager data that includes customer names and telephone numbers, and called and calling number data.

With the following features, healthcare providers can protect patient privacy and demonstrate the compliance with HIPAA.

Table 36: Communication Manager security and compliance of HIPAA

Feature	How related to HIPAA	Where documented
Encryption	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate	• Encryption overview on page 37
System access control	Implement technical policies and procedures for electronic information systems that maintain electronically-protected health information to permit access only to those persons or software programs that have been granted access rights.	• Managing Communication Manager accounts on page 83
Authentication	Implement procedures to verify that a person or entity seeking access to electronically-protected health information is the one claimed.	• Access profiles on page 31 • Managing Communication Manager accounts on page 83
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.	• Managing Communication Manager accounts on page 83

Considerations for customers who must comply with CALEA

Note:

This law applies to U.S. customers only. Customers must seek appropriate legal advice for interpretation of the requirements of this act. 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, the Congress in America 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 makding 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. The following are some examples of such products:

- NexTone
- AcmePacket
- Sipera

In addition, the following characteristics of Communication Manager aid in CALEA compliance:

- 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 divided into call control signals and bearer signals. This simplifies the task of determining what data to monitor.
- Assurance of the authenticity and integrity of the calls being monitored through encryption and authentication capabilities of Communication Manager.
- Call Detail Records, which records called numbers, and other call data that can be useful to law enforcement agencies.
- The Service Observing feature of Communication Manager that permits monitoring of calls with or without the knowledge of the parties on the call.

Considerations for customers who must comply with FISMA

Note:

This law applies to U.S. customers only. Customers must seek appropriate legal advice for interpretation of the requirements of this act. 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 network.

For more information of features related to system security, see the table on page 150.

Table 37: Communication Manager security and compliance of FISMA

Feature	How related to FISMA	Where documented
Encryption	Transmitted data is protected from packet-sniffing and eavesdropping and other unauthorized access.	See: • Encryption overview on page 37
System access control	Access to data is protected from unauthorized personnel	See: • Managing Communication Manager accounts on page 83
Authentication	Access to the system is restricted by login/password.	See: • Administration of authentication passwords on page 84
Logging	Security-related events are logged	See: • Configuration of SNMP and syslog on page 88
Firewall	Access to Communication Manager network is protected	See: • Firewall protection on page 25
Backup of data	Data saved on backup or backup server. Protected by encryption and key	See • Secure backups of Communication Manager data and translations on page 156
Toll fraud prevention	Unauthorized use of long-distance is prevented	See • Limitation of long distance access on page 87

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. The suggested controls are not mandatory, however, an organization that prefers not to implement the suggestions must explain the decision to not implement the suggested controls.

See the table on page 151 on how ISO 17799 addresses the different categories of data security management.

Table 38: Communication Manager security and compliance of ISO 17799

ISO 17799 Security Guidelines	Communication Manager features and processes
Ensure that applications process information correctly	
• Use validation checks to control processing	Use the System Log and Maintenance Alarm and Event logs. See: • Configuration of SNMP and syslog on page 88
• Validate data input into your applications	Communication Manager can track administration and notify the administrator when changes are made. Use the System Log, and the Maintenance Alarm and Event logs. See: • Configuration of SNMP and syslog on page 88 • Maintenance Procedures for Avaya Aura® Communication Manager, Gateways and Servers (03-300432) • Maintenance Commands for Avaya Aura® Communication Manager, Gateways and Servers (03-300431)
• Protect message integrity and authenticity	Use digital certificates when transmitting data to ensure authorization. Restrict access to the system with logins, passwords, and authentication keys. See: • Chain of trust on page 63 • Administration of authentication passwords on page 84
• Validate your applications' output data	Use audits and status reports to verify output. See: • Maintenance Procedures for Avaya Aura® Communication Manager, Gateways and Servers (03-300432) • Maintenance Commands for Avaya Aura® Communication Manager, Gateways and Servers (03-300431)

ISO 17799 Security Guidelines	Communication Manager features and processes
• Use cryptographic controls to protect your information	Encrypt data to protect data from packet-sniffing and eavesdropping. See: • Encryption overview on page 37 • Secure updates of Avaya software and firmware on page 157
Protect and control your organization's system files	
• Control the installation of operational software	Communication Manager requires the appropriate access control to install software. In addition, a digital certificate from the software ensures the software is permitted to be installed on the server. See • Security problems addressed by digital certificates on page 30 • Secure updates of Avaya software and firmware on page 157
• Control the use of system data for testing	Avaya uses internal ISO-certified testing processes for software.
• Control access to program source code	Communication Manager source code is unaccessible outside of Avaya. The Linux operating system is also restricted. See • Linux as the chosen operating system for Communication Manager on page 23
Control development and support processes	
• Establish formal change control procedures	Avaya uses internal ISO-certified change control processes for software. For security-related updates, Avaya uses a change policy as documented in Classification of security updates on page 140.
• Review applications after operating system changes	Avaya uses internal ISO-certified test procedures after operating system changes. See Validation of a security update on page 141.
• Restrict changes to software packages	Avaya includes only the Linux software packages it needs for Communication Manager. Communication Manager software is proprietary, and Linux software cannot be changed on an installed system. Standard program binaries are normally installed with write permissions only to the super-user (root) and cannot be modified.
• Prevent information leakage	Communication Manager does not have antivirus, antiworm, or antitrojan software. However, Avaya does

ISO 17799 Security Guidelines	Communication Manager features and processes
	not recommend using third-party antivirus software on Communication Manager. For more information, see Protection from viruses and worms on page 27.
• Control outsourced software development	Avaya software, if outsourced, is developed according to Avaya's ISO-certified processes.
Control your technical system vulnerabilities	Communication Manager offers many features and processes to protect the customer's communications network. See: • Encryption overview on page 37 • Managing Communication Manager accounts on page 83 • Configuration of SNMP and syslog on page 88 • Chain of trust on page 63 • Avaya Public Key Infrastructure on page 63 • Configuration of SNMP and syslog on page 88 • Secure backups of Communication Manager data and translations on page 156 • Secure updates of Avaya software and firmware on page 157

Considerations for customers who must comply with E911

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 Rule making. 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.

Note:

This law applies to U.S. customers only. Customers must seek appropriate legal advice for interpretation of the requirements of this act. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

However, the Occupational Safety and Health Administration (OSHA) can interpret 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 might cause, or are likely to cause, death or serious physical harm.

In addition, there are approximately 17 states with current or pending legislation requiring enterprise switches to be able to dial 911 and report the number of the caller, 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 a routing table to send the emergency call over an ISDN trunk and include the Calling Party Number for automatic identification by Public Safety Answering Point (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 PSAP through a Centralized Automatic Message Accounting (CAMA) trunk, which sends Caller Emergency Service Identification (CESID) to 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 appropriate PSAP receives the 911 call and location identification.

IP telephony

For IP telephones, SIP-enabled telephones, or softphones, all of which do not have a physical connection to the Communication Manager server or gateways but access the communications system over 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. In the case of softphones, Communication Manager also permits the user to enter a telephone number which the PSAP can then use to identify the location of the user 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. For more information about how the RedSky products interacts with the E911 capabilities of Communication Manager, log on to http://www.redskytech.com. For more information on the 911 and E911 capabilities of Communication Manager, 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 telephone 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, customers must be educated 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:

- The security properties of products are evaluated by competent and independent licensed laboratories.
- 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 Server S8710.

- Avaya Branch Gateway 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 Server S8510.
- 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 Server S8510.

The CC web portal (http://www.commoncriteriaportal.org/index.html) reports the status of the CCRA, the CC and the certification schemes, licensed laboratories, certified products and related information, news, and events.

Secure backups and updates

Secure backups of Communication Manager data and translations

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 to restore the data. The password is not retrievable from Communication Manager.
- The use of a 15-character to 256-character passphrase for encryption of the backup of data.

For more information on backing up data with Communication Manager, see *Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300432.

Note:

You can backup and restore data of the G250, G350, G430, and G450 Branch Gateways using a single CLI command for backup and a single CLI command for restore.

For information on backup and restore with Gateways, see:

- *Administration for the Avaya G250 and Avaya G350 Branch Gateway*s, 03-300436
- *Administering Avaya G430 Branch Gateway*, 03-603228
- *Administering Avaya G450 Branch Gateway*, 03-602055

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. For more information, see *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 Branch 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 is displayed with an option to continue the installation. For more information, see *Firmware Download Instructions*.

When an Avaya server serves as a repository from which other Avaya devices download software or firmware, the server provides a certificate for authentication to the downloading device. When IP telephones attempt to download firmware from a Communication Manager server over a TLS session, the server provides a certificate for authentication. For more information, see *Downloading Avaya 46xx IP Telephone Software Using Avaya Media Servers*.

Communication Manager uses the Secure Copy Protocol (SCP) to transfer files between a software repository and a Communication Manager server or between a Communication Manager server and other Avaya devices. SCP ensures that the file transfer is secure.

Remote monitoring and maintenance

Avaya offers Secure Access and Control (SAC) monitoring and maintenance services. SAC uses both Secure Services Delivery Platform (SSDP) and the Secure Services Gateway (SSG) to provide a secure platform from which remote technicians and Expert Systems^{SM} access products at customer sites for security audits such as perimeter scans and penetration tests, and to update firmware and resolve alarms. Using IP connectivity, SAC offers service at two levels:

- **SAC Basic**: SAC Basic collects alarms from Avaya Products and sends the alarms to Avaya over a B2B VPN/Frame Relay link. The firewall of the customer organization and SSDP control inbound access to Avaya products.
- **SAC Premium: SAC Premium** builds on SAC Basic by adding inbound gateway functionality to the SSG. The customer uses the SSG to control and supervise Avaya's access to the customer network and products and to record the following:
    - What product was accessed
    - Who accessed the product
    - When was the product accessed
    - Why was the product accessed

Only authorized Avaya maintenance technicians have access to customer data that is needed to perform maintenance on customer products. SSDP logs the user, time and type of access, as well as the reason for the access using the Trouble Ticket number.

SSDP firewall and wireless access

Avaya uses a firewall/VPN product called Secure Gateway 2000, formerly a VPNet product, on the B2B link. This IPSec, 3DES VPN firewall interoperates with other VPN firewall vendors products such as Cisco, Nortel, and NetScreen.

The firewall protects the DMZ from the rest of the Avaya network. Additional firewalls and intrusion detection systems are deployed throughout the Avaya network to block customer servers from other Avaya users.

Remote laptops and desktops use a VPN client to gain wireless access to the Avaya network. The remote devices must first connect to the WEP-protected WLAN, then the devices are authenticated on the VPN network, and then on the Avaya LAN network.

Remote technicians first access the Avaya LAN using VPN clients, then the Single Sign-On technology of SSDP authenticates the technician. 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 Avaya 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 e-mail 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: Servers

Avaya-certified servers

Avaya Aura® Communication Manager supports the following servers:

- S8300D
- S8510
- S8800
- HP ProLiant DL360 G7 1U
- Dell™ PowerEdge™ R610 1U
- HP ProLiant DL360p G8
- Dell™ PowerEdge™ R620

For information about the supported servers, see *Avaya Aura® Communication Manager Hardware Description and Reference,* 555-245-207.

Appendix B: Network Services On Communication Manager Servers

Network services on Communication Manager servers

Network service and port information for S8510 series server and duplicated series server can be obtained from the Avaya Support website http://support.avaya.com.

Appendix C: Additional Security Resources

Security documents on the Avaya Support website

Security-related documents that complement this security guide are listed in the table on page 163.

Table 39: Security related Communication Manager documents

Document title	Link
Access Security Gateway family of security products	http://support.avaya.com/japple/css/japple?PAGE=Product&temp.productID=107697.
Application Note: G350 and G250 R3.0 IPSec VPN	http://support.avaya.com/elmodocs2/g350/AppNotes_G350_G250_R3_ndezent_070605.pdf
Avaya Enterprise Services Platform Security Overview	Requires non-disclosure agreement
Avaya Interactive Response Security	http://support.avaya.com/elmodocs2/ir/r2_0/print_Security.pdf
Avaya's Security Vulnerability Classification	http://support.avaya.com/elmodocs2/security/security_vulnerability_classification.pdf
Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework	http://www.bis.org/publ/bcbs128.pdf
Avaya Aura® Communication Manager Administrator Logins	http://support.avaya.com
Downloading Avaya 46xx IP Telephone Software Using Avaya 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

Document title	Link
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

Appendix D: Communication Manager Web Access Mask Default Settings

Communication Manager Web Access Mask default settings

Table 46: Communication Manager Web Access Mask default settings on page 175 on page 165 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 and a blank indicates that the user has no access to the page.

Table 40: Communication Manager Web Access Mask default settings

Menu-Item	Fixed (suser)	Editable (user)
	Profile 18	Profile 19
Administration		
Licensing	X	X
Feature Administration	X	X
Messaging	X	X
Native Configuration Manager	X	X
Alarms		
Current Alarms	X	X
Agent Status	X	
SNMP Agents	X	
SNMP Traps	X	
Filters	X	
SNMP Test	X	
Diagnostics		
Restarts	X	X
System Logs	X	X

Menu-Item	Fixed (suser)	Editable (user)
	Profile 18	Profile 19
Ping	X	
Traceroute	X	
Netstat	X	
Server		
Status Summary	X	X
Process Status	X	
Interchange Servers	X	
Busy-Out/Release Server	X	
Shutdown Server	X	
Server Date/Time	X	
Software Version	X	X
Server Configuration		
Server Role	X	
Network Configuration	X	
Duplication Parameters	X	
Static Routes	X	
Display Configuration	X	
Server Upgrades		
Pre Update/Upgrade Step	X	
Manage Updates	X	
IPSI Firmware Upgrades		
IPSI Version	X	X
Download IPSI Firmware	X	
Download Status	X	
Activate IPSI Upgrade	X	
View IPSI Version results	X	
Activation Status	X	
Data Backup/Restore		
Backup Strategies	X	X
Backup Now	X	X

Menu-Item	Fixed (suser)	Editable (user)
	Profile 18	Profile 19
Backup History	X	X
Schedule Backup	X	
Information found in backup logs	X	
View/Restore Data	X	
View.Restore data results	X	
Restore History	X	
Security		
Administrator Accounts	X	
Login Account Policy	X	
Change Password	X	X
Login Reports	X	
Server Access	X	
Syslog Server	X	
Authentication File	X	X
Firewall	X	
Installing Root Certificates using IE	X	X
Trusted Certificates	X	
Server/Application Certificates	X	
Certificate Alarms	X	
Certificate Signing Request	X	
SSH Keys	X	
Web Access Mask	X	
Miscellaneous		
File Synchronization	X	
File Synchronization Status		
Download Files	X	
Download File Results	X	
Avaya Aura® CM Telephone Message File	X	
Multiple Avaya Aura® CM Telephone Message File	X	
Messaging Software	X	

Menu-Item	Fixed (suser)	Editable (user)
	Profile 18	Profile 19
Server Field Definitions	X	X

Index