



**Avaya Aura® Messaging Security
Design**
Release 6.1

December 2011

Notice

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

Documentation disclaimer

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

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: <http://www.avaya.com/support>. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by the said Avaya reseller and not by Avaya.

Licenses

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

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

License types

- Designated System(s) License (DS):
End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- Concurrent User License (CU):
End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the

Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

- Named User License (NU):
End User may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User" means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (for example, webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR):
Customer may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License"). (See Third-party Components for more information).

Copyright

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

Third Party Components

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

Preventing toll fraud

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

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site:

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

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

Trademarks

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

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

Downloading documents

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction.	9
Information classifications and NDA requirements	9
Disclaimer	10
Document structure	11
Messaging security philosophy overview	11
Messaging security responsibility	12
Responsibility for security updates	13
Related documents	13
Chapter 2: Messaging Security overview	15
Secure by design	15
Secure by default	15
Secure communications.	16
Operating system hardening	17
Benefits of Linux operating system for Messaging	17
Modifications to the Linux OS to improve security	17
RPMs removed	17
Unnecessary IP ports closed	18
Firewall protection	18
Drive partitioning.	18
Linux OS kernel hardening	18
Privilege escalation and root logins	19
Access Security Gateway	19
Benefits of SSH/SCP over Telnet, FTP and SNMP	19
Disabled by default	19
Avaya Services.	20
Planning against viruses and worms and other malicious code	20
DoS methods Avaya has designed against	21
Security problems addressed by digital certificates	23
Additional information.	24
Secure administration	24
Access profiles.	24
System Management Interface default profiles and permissions	24
System Management Interface profiles.	24
System Management Interface default settings	25
Privilege escalation	32
Additional information.	32
Local host account authentication	33

Chapter 3: Configurable Security	35
Configurable encryption.	35
Avaya's encryption overview	35
Transport and storage encryption algorithms	36
SRTP media encryption for SIP Integration	36
Encryption summary.	37
Mixing encrypted and nonencrypted policies	40
Authentication files for Messaging	40
About the authentication file	40
ASG	41
Starting the AFS application	41
Creating an authentication file for a new system	41
Creating an authentication file for a file replacement	42
Creating an authentication file for an upgrade to a new major release	44
Obtaining the AFID from System Platform Web console	45
Obtaining the AFID from Messaging SMI.	45
Installing an authentication file	45
Digital certificates and server trust relationships	46
Chain of trust.	46
Avaya Public Key Infrastructure	47
Avaya security certificate types.	48
Avaya certificate repository	49
PKI in Messaging	49
Install Root Certificate on a PC	50
Installing a Root Certificate on a PC	50
Trusted certificates	51
Displaying a trusted certificate on the server	51
Adding a trusted certificate to the server	51
Deleting a trusted certificate from the server	51
Removing a trusted certificate on the server from a particular repository	52
Copying a trusted certificate on the server from one repository to another repository	52
Server and application certificates	52
Displaying a server or application certificate	53
Adding a server or application certificate to the server.	53
Removing a server or application certificate from the server	54
Copying a server or application certificate to different repository on the same server	54
Customers can install their own trusted certificates	54
Third-party certificate management	55
Connection to Messaging Web interface.	56

Managing changes to the Avaya certificate	56
Certificate alarms	57
Creating certificate alarms	57
Additional information.	58
Administrative accounts	58
Credentials complexity and expiration requirements	58
Password complexity policies	59
Credentials expiration and lockout policies	59
Password administration recommendations.	61
Credentials management	61
More information.	61
Applying profiles for role-based administration.	61
Creating the privileged administrator account.	62
Managing administrative accounts	64
Account administration recommendations	65
Administering authentication passwords	65
Access Security Gateway (ASG)	66
ASG Guard and ASG Guard Plus	66
ASG Guard II	67
ASG Guard and ASG Guard II compared.	67
ASG security products	68
Managing subscriber accounts	68
Limiting client access	68
Telephone user interface (TUI) access	69
Client IP network access	69
E-mail clients via IMAP4.	69
Web browser (for User preferences)	70
Lightweight Directory Access Protocol client access.	70
Subscriber mailbox password administration	70
Toll fraud prevention.	71
Limiting long distance access	72
Configuring logging and events	72
Configuring SNMP and syslog	73
What security-related events are logged?	73
Configuring SNMP in Messaging	74
Agent Status page	74
SNMP Agents page	74
SNMP Traps page	75
Re-enable SNMP agent	75
Messaging security event notifications through SNMP.	75

Configuring the syslog server in Messaging.	75
General syslog guidelines.	76
Administering the syslog server in Messaging	76
Accessing system logs through the Web	77
More information.	77
Chapter 4: Network Security Integration	79
Network "best practices"	79
Separation of network functionality	79
Control and bearer signaling in VLANs	79
Layer 2 and Layer 3 hardening	80
Designing VLAN groups for functional network segmentation.	80
Traffic filtering and firewalling between VLANs	81
How ARP spoofing facilitates network attacks	81
Security strategies to combat ARP spoofing	82
Security vulnerabilities with name and address management	82
DNS vulnerabilities.	83
DNS security	83
How Messaging addresses NIST recommendations	83
Confidentiality and privacy	83
Switch default password vulnerability	84
Classical wiretap vulnerability	84
ARP cache poisoning and ARP floods	85
Web server interfaces	85
Integrity issues.	85
Availability and Denial of Service.	86
Default password vulnerability	86
Account lockout vulnerability.	86
Chapter 5: Operational Security	87
Avaya Security Advisories	87
What is an Avaya Security Advisory	87
How do I get Avaya Security Advisories?	88
How to interpret an Avaya Security Advisory	89
How an advisory is organized.	90
How Avaya incorporates security updates in its applications	91
Logging, monitoring and audit trails	91
Removing old accounts	92
Restricting web access to system logs	92
Where is security information logged?.	92

Reading and interpreting the security logs	93
Interpreting the syslog header	93
Syslog header example	93
Syslog server example for a branch gateway	94
Interpreting SNMP entries in the syslog	94
SNMP log example	95
Interpreting the platform command history log	95
Platform command history log example	96
Software and firmware updates.	96
How Avaya delivers security updates	96
Validating a security update.	98
Applying an operating system security update	98
Applying an Avaya field load or software update	99
Determining the contents of a security update	99
Considerations for customers who must comply with the Sarbanes-Oxley Act.	100
Messaging data used for financial purposes	102
Other adjunct systems collecting Messaging data	102
Considerations for customers who must comply with the Graham-Leach-Bliley Act.	103
Considerations for customers who must comply with HIPAA	104
Considerations for customers who must comply with CALEA.	105
Considerations for customers who must comply with FISMA	106
Considerations for customers who want to comply with ISO 17799.	107
Considerations for customers who must comply with E911	110
Messaging compliance with 911	111
Traditional telephony	111
IP telephony	111
Considerations for non-US customers who must comply with regulations . .	111
Basel II	112
Common Criteria.	112
Secure backups and updates	113
Secure backups of Messaging data and translations	113
Secure updates of Avaya software and firmware	113
Remote monitoring and maintenance	114
SSDP firewall and wireless access	114
Remote password complexity and expiration parameters	115

Appendix A: Physical interfaces and associated network services . . 117

Appendix B: Internet ports and protocols. 119

Appendix C: Additional security resources. 125

 Security documents on the Avaya Support site 125

Index 127

Chapter 1: Introduction

Information classifications and NDA requirements

This document provides security-related information for Avaya Aura® Messaging. For information on the four types of information classifications, see [Table 1: Avaya information classifications](#) on page 9

This document contains confidential information. You must not share this confidential information with unauthorized individuals or post the information on a public Web site. While there are references to additional information sources throughout this document, some sources disclose confidential and proprietary information and require a nondisclosure agreement (NDA) with Avaya.

Table 1: Avaya information classifications

Classification	Description
Avaya Restricted	For extremely sensitive business information, intended strictly for use within Avaya. Unauthorized disclosure of this information can have a severe adverse impact on Avaya, its customers, BusinessPartners, and suppliers.
Avaya Confidential	For less sensitive business information intended for use within Avaya. Unauthorized disclosure of this information can have significant adverse impact on Avaya, its customers, BusinessPartners, and suppliers. This classification contains information that some people may consider as private.
1 of 2	

Table 1: Avaya information classifications

Classification	Description
Avaya Proprietary	For other information that does not classify as Avaya Restricted information or Avaya Confidential information. While disclosure might not have a serious adverse impact on Avaya, its customers, BusinessPartners, and suppliers, this information belongs to Avaya, and unauthorized disclosure is against Avaya policy.
Public	For information explicitly approved by Avaya management as nonsensitive information available for external release.
2 of 2	

Disclaimer

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

Document structure

Table 2: Components of the the Messaging Security Design guide

Chapter	Description
Introduction	• Messaging security philosophy overview on page 11 • Related documents on page 13
Messaging Security overview	Describes the security features of Avaya products.
Configurable Security	Describes the security issues in Avaya products that you can enable for additional security.
Network Security Integration	'Describes the method to securely integrate Avaya products to an existing network by leveraging resources such as Lightweight Directory Access Protocol (LDAP), active directory, and firewall.
Operational Security	Discusses ongoing activities useful to ensure a high level after the solution has been deployed. Areas include patching, logging, and monitoring.
Appendices	– Appendix A: Physical interfaces and associated network services on page 117. – Appendix B: Internet ports and protocols on page 149. – Appendix C: Additional security resources on page 125.

Messaging security philosophy overview

This document describes security-related considerations, features, and services for Messaging and its servers. To prevent malfunction or theft of service, a Messaging solution must be secure from the following types of security threats:

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

Messaging security responsibility

Avaya is responsible for designing and testing its products for security. When Avaya sells a product as a hardware/software package, Avaya's design and testing includes the operating system. In this case, Avaya may modify the operating system to improve system operation or to resolve a security vulnerability.

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

No telecommunications system can be entirely free from the risk of unauthorized use.

Customers have ultimate control over the configuration and use of the product. They are solely responsible for ensuring the security of their systems is adequate for their intended use.

Customers administer their system configuration and can tailor that system to meet their unique needs but must also ensure to their own satisfaction that the security configuration is aligned with appropriate risk management best practices. Customers are responsible for keeping themselves informed of the latest information for configuring their systems to prevent unauthorized use.

System managers and administrators are responsible for obtaining and acting on all recommendations, installation instructions, and system administration documents provided with the product. This information can help them understand the features that might introduce risk of toll fraud and the steps they must take to reduce that risk. Responsibilities owned by system managers include (but are not limited to):

- Integration of Messaging servers into existing TCP/IP network(s) according to the corporate networking policies. In most cases, existing firewalls, and corporate security policies and practices can be implemented or adapted for the Messaging system.
- Careful consideration for the security implications when the client access to the Messaging system are enabled.
- Protection of server against unauthorized use with appropriate administrator and user passwords. Use longer and more random passwords to minimize the possibility of compromise. Ensure that you secure the passwords properly.
- Protection of the surrounding network to minimize the threat of denial of service attacks.
- Review of server logs to detect actual and attempted unauthorized use and to identify its source.

System managers are also responsible for: Physical security, password protection, password control, backups, environmental controls.

Neither Avaya nor its suppliers or business partners can guarantee that any product is immune from risk of unauthorized use of IP or telecommunications services or facilities accessed through or connected to this product. Avaya is not responsible for any damages or charges that result either from unauthorized usage or from incorrect installation of the security patches that are made available periodically. See the End-User License Agreement(s) associated with your Messaging product(s) for additional details.

Responsibility for security updates

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

Avaya notifies customers of the availability of security updates through Security Advisories. Customers can subscribe to be notified about Security Advisories by email. See [What is an Avaya Security Advisory](#) on page 87 and [How do I get Avaya Security Advisories?](#) on page 88.

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

Related documents

This document describes security related features of messaging, messaging servers, telephones and media gateways.

This descriptive document belongs to a set of documents that describe potential security risks to Avaya products, and the features that Avaya provides to prevent security related threats. This document contains references to other documents for procedures to configure and use 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, Web Conferencing, Voice Monitoring Manager, and Provisioning and Installation manager.

Chapter 1: Introduction

- Secure gateways and C360 stackable switches

Avaya Toll Fraud Security, available at <http://support.avaya.com> describes the high-level security risks and mitigating features offered by the body of Avaya products. This guide seeks to provide background descriptions of IP telephony security risks and to briefly identify security features commonly implemented within Avaya's product line.

Chapter 2: Messaging Security overview

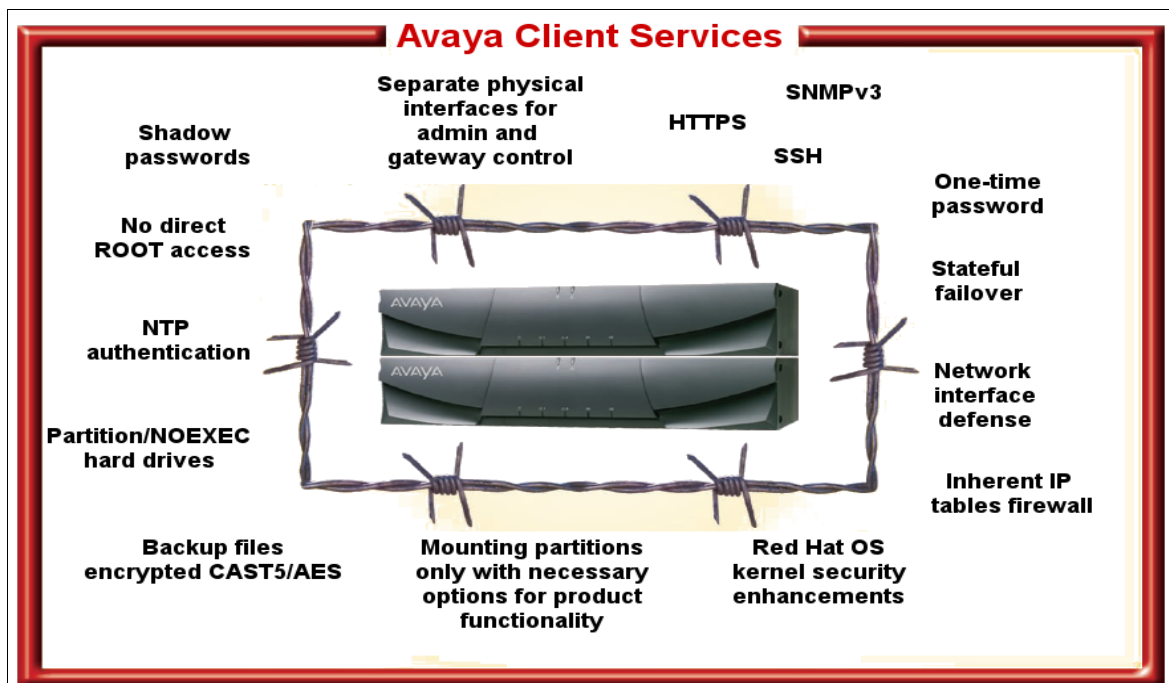
Secure by design

Secure by design encompasses a security design strategy that enables separation of communication services from the enterprise production network and minimal exposure of additional services by communications servers. Avaya products conform to a comprehensive set of security guidelines and best practices to meet your expectations. Avaya updates the security guidelines and best practices annually to align with your requirements of security features for unified communications products.

Secure by default

Secure by default, the Avaya second security layer, incorporates a hardened Linux operating system with inherent security features for Avaya Media Servers with Messaging. Avaya modifies the Linux kernel for secure, real-time telephony processing. The hardened Linux OS provides functions required to support core applications. These OS functions secure mission-critical call processing applications and protect you from toll fraud and other malicious attacks.

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



Messaging provides a range of inbuilt functions, which protect against threats from malicious software. These inbuilt functions minimize the need for a dedicated antivirus software that may reduce call processing efficiency and require attention to ensure the antivirus database is updated.

Secure communications

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

Critical adjunct connections like the CTI link can be isolated to a dedicated security zone and encrypted.

Operating system hardening

- [Benefits of Linux operating system for Messaging](#) on page 17
- [Benefits of SSH/SCP over Telnet, FTP and SNMP](#) on page 19
- [Planning against viruses and worms and other malicious code](#) on page 20

Benefits of Linux operating system for Messaging

The open source Linux operating system provides a secure foundation for communications

Benefits of the open source foundation include:

- Security experts worldwide review the source code looking for defects or vulnerabilities.
- Avaya engineers monitor and review Linux OS enhancements developed by the Linux community to incorporate the enhancements in Avaya products.
- Linux based Avaya servers and gateways protect against DoS attacks such as SYN floods, ping floods, malformed packets, oversized packets, and sequence number spoofing.

Note:

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

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

Modifications to the Linux OS to improve security

Avaya has modified, or 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, uninstall, verify, query, and update software packages.

Avaya IP telephony application requires approximately 30% of the up to 800 distributed RPMs in the Linux OS distribution. To improve efficiency and security, Avaya removes the unused RPMs from the Linux OS distribution. For example, tcpdump packet capturing tools.

To view the list of RPMs Avaya employs, run the following command at the Messaging server's command line interface (CLI): **rpm -qa**

Unnecessary IP ports closed

Many Linux modules like SSH or Apache or SSL/TLS (HTTPS) are applications that open Ingress network services. Avaya reduces the Ingress network services only to those that are necessary for its telephony applications, thus minimizing exposure of the operating system to network-based attacks. Avaya disables by default less secure network services like TELNET and FTP (see [Benefits of SSH/SCP over Telnet, FTP and SNMP](#) on page 19), although customers can enable these services as needed. The customer can enable the FTP Server, Telnet Server, SAT (Telnet 5023) and disable SSH Server, High Priority SSH, and SAT (SSH 5022) using the SMI - Administration > Server(Maintenance) > Security > Server Access page.

Firewall protection

The IPTables firewall protects Avaya products from network based attacks. The firewall also protects against Ingress services that the XINETD mechanism enables. The XINETD mechanism monitors connection requests on specific ports and starts server programs to perform services associated with those specific ports

The Messaging System Management Interface manages the host based IPTables firewall, which allows you to control the ports to accomodate your network security requirements.

Drive partitioning

File and directory permissions minimize access as much as possible and act as a preventive measure against malware and tampering. See [Planning against viruses and worms and other malicious code](#) on page 20:

- Separate hard drive partitions to store executable files and data.
- Execute permissions disabled in hard disk partitions which contain data.

Linux OS kernel hardening

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

Privilege escalation and root logins

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

**Tip:**

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

Access Security Gateway

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

Benefits of SSH/SCP over Telnet, FTP and SNMP

Connection protocols that send data - especially logins and passwords - in plaintext, that is, unencrypted or "in the clear," can pose a serious security risk to a VoIP enterprise. Protocols such as SSH and SFTP that encrypt data ensure critical data is protected. Due to new legislation and stricter auditing requirements, Avaya implements more secure protocols in the secure connection design.

Disabled by default

By default, Avaya disables these inherently insecure network services:

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

Note:

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

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

- Secure Shell (SSH)
- Secure Copy (SCP) or Secure File Transfer Protocol (SFTP)
- SNMP with these stipulations:
 - SNMPv3 is the preferred version due to its built-in security mechanism.
 - SNMPv1 or v2c, while supported, provide only a limited security capability based on community names:
 - The community name for SNMPv1 and SNMPv2c is protected when accessing writable MIBs.
 - For read-only MIBs SNMPv1 and SNMPv2c community names are unprotected.SNMP security secrets (for example, community strings) are customer-administrable.
- Other protocols protected using a Transport Layer Security (TLS) or Internet Protocol Security (IPSEC) connection

Avaya Services

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

Planning against viruses and worms and other malicious code

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

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

A virus infects a system through a host. For example, an application, an e-mail, or a file. A user action spreads the virus in a system. For example, opening an infected e-mail attachment. A worm does not require a host or a user action to infect a system. See [Table 3: Security impacts from viruses and worms](#) on page 21 for more information.

Table 3: Security impacts from viruses and worms

Security implementation	Security impact
Natural immunity	Avaya's Linux-based servers <i>do not</i> 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 super user is the sole user with write permissions to standard program binaries. These write permissions to standard program binaries cannot be modified. Restricting write permissions to the super user results in limited virus infections in Linux OS.
Antivirus products	Avaya products are inherently secure against virus infections. You may use third party antivirus products. To ensure minimal impact to the end user, scan the system with the third party antivirus product when there is minimal load on the server.
Firewall	Unused ports are closed off, thereby reducing the attack surface.
Logs	Exhaustive logging allows malicious activity to be detected.
Access profiles	Provide granular control of admin user privileges.

DoS methods Avaya has designed against

A DoS attack occurs when an attacker attempts to flood a resource with data and requests which denies legitimate users access to the resource, or prevents the resource from processing legitimate requests. Regardless of the method, the net effect of DoS attacks is to shut down a server or an application.

Messaging servers survive DoS attacks listed in [Table 4: Avaya's design against types of DoS attacks](#) on page 22 without loss of sanity, without rebooting or restarting, and without reloading, and automatically recover to full service after the DoS attack.

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

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

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

Attack type	Description
Finger of death	The attacker sends finger requests to a specific computer every minute but never disconnects. Failure to terminate the connection can quickly overload the server's process tables. The finger listen port number is 79 (see RFC 742).
Chargen packet storm	The attacker spoofs the chargen service port 19 between services installed on different computer systems. Spoofing causes the services to go in an infinite processing loop. The infinite loop results in loss of performance or total shutdown of affected network segments.
Malformed or oversized packets	Malformed packet attacks cause protocol handlers to cease operation. The protocol handlers fail to process odd formations of a protocol or malformed packets sent as part of a protocol. Oversized packets place data in an order that the protocol handlers do not recognize or create packets that are larger than the maximum allowed size.
SPANK	The target responds to TCP packets sent from a multicast address causing a DoS flood on the target's network.
SNMP PROTOS	Utilizing the Protos SNMP tool to test SNMP code, an attacker can generate thousands of valid SNMP packets with strange and anomalous values that cause error conditions. (See http://www.ee.oulu.fi)
2 of 2	

Security problems addressed by digital certificates

Generally, digital certificates provide:

- Secure authentication: The sender and the recipient validate each other's public key and, therefore, validate each other.
- Data integrity: The data exchanged between the sender and recipient is digitally signed. The recipient host validates the digital certificate to determine that the data is not modified.

Messaging uses digital certificate when establishing:

- an HTTPS connection to the Apache Web server for the Messaging web interface
- SIP-TLS connections
- IMAPS connection
- LDAPS connection

Additional information

- [Avaya Public Key Infrastructure](#) on page 47
- [Secure updates of Avaya software and firmware](#) on page 113

Secure administration

- [Access profiles](#) on page 24

Access profiles

Access to Messaging, its underlying operating system, and its hardware components (for example, media gateways and IP telephones) is through the System Management Interface which permits:

- Access to system alarms, logs, and diagnostics
- Messaging and media gateway configurations
- Security access, configuration, and monitoring.

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

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

- [System Management Interface default profiles and permissions](#)

System Management Interface default profiles and permissions

System Management Interface profiles

[Table 5: Messaging System Management Interface default profiles](#) on page 25 lists and describes the intended use of the default profiles for the System Management Interface.

Note:

Members of the suser s Linux group have full access to all Web pages. Members of the user s have access to a limited subset of these pages.

Table 5: Messaging System Management Interface default profiles

Profile number	Group	Description
0	suser	Highest level services access; requires secondary user authentication.
1	suser	Designated for service management; requires secondary user authentication.
2	suser	Designated for Avaya 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 Profile 18. Designated for telephony administrators who need lower-level access and functionality.
20-69		Available for customer modification

System Management Interface default settings

Access permissions to the System Management Interface are administered on the **Security > Web Access Mask** page. [Table 6: Messaging Web Access Mask default settings](#) on page 26 lists the default access settings for all Messaging System Management Interface for Profile 18 and Profile 19. The “X” indicates that the user has access to the corresponding page; a blank denies access to the page.

Avaya recommends you use Profile 18 and Profile 19 as the base profile to create new user profiles. Add or restrict users' permissions to pages according to your RBAC or individual security policy..

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

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

Table 6: Messaging Web Access Mask default settings

Menu-Item	Fixed (suser)	Editable (user)
	Profile 18	Profile 19
Administration		
Licensing	X	X
Messaging	X	X
Server (Maintenance)	X	X
Alarms		
Current Alarms	X	X
Agent Status	X	
SNMP Agents	X	
SNMP Traps	X	
Filters	X	
SNMP Test	X	
Diagnostics		
System Logs	X	X
Ping	X	
Traceroute	X	
Netstat	X	
Server		
Status Summary	X	X
Process Status	X	
Shutdown Server	X	
Server Date/Time	X	
1 of 7		

Table 6: Messaging Web Access Mask default settings

Menu-Item	Fixed (suser)	Editable (user)
	Profile 18	Profile 19
Software Version	X	X
Server Configuration		
Network Configuration	X	
Static Routes	X	
Display Configuration	X	
Server Upgrades		
Manage Updates	X	
Data Backup/Restore		
Backup Now	X	X
Backup History	X	X
Schedule Backup	X	
Backup Logs	X	
View/Restore Data	X	
Restore History	X	
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	
2 of 7		

Table 6: Messaging Web Access Mask default settings

Menu-Item	Fixed (suser)	Editable (user)
	Profile 18	Profile 19
Install Root Certificate	X	X
Trusted Certificates	X	
Server/Application Certificates	X	
Certificate Alarms	X	
Certificate Signing Request	X	
SSH Keys	X	
Web Access Mask	X	
Miscellaneous		
Download Files	X	
Licensing		
License Status	X	X
Messaging System (Storage)		
User Management	X	
Class of Service	X	
Sites	X	
Topology	X	
Storage Destinations	X	
System Policies	X	
Enhanced List Management	X	
System Mailboxes	X	
System Ports and Access	X	
User Activity Log Configuration	X	
Reports (Storage)		
Users	X	
3 of 7		

Table 6: Messaging Web Access Mask default settings

Menu-Item	Fixed (suser)	Editable (user)
	Profile 18	Profile 19
Info Mailboxes	X	
Remote Users	X	
Uninitialized Mailboxes	X	
Login Failures	X	
Locked Out Users	X	
Server Information		
System Status (Storage)	X	
System Status (Application)	X	
Alarm Summary	X	
Voice Channels (Application)	X	
Cache Statistics (Application)	X	
Server Settings (Storage)		
External Hosts	X	
Trusted Servers	X	
Networked Servers	X	
Request Remote Update	X	
IMAP/SMTP Settings (Storage)		
General Options	X	
Mail Options	X	
IMAP/SMTP Status	X	
Telephony Settings (Application)		
Telephony Integration	X	
Server Settings (Application)		
Dial Rules	X	
4 of 7		

Table 6: Messaging Web Access Mask default settings

Menu-Item	Fixed (suser)	Editable (user)
	Profile 18	Profile 19
Cluster	X	
System Parameters	X	
Languages	X	
Log Configuration	X	
Advanced (Application)		
System Operations	X	
Timeouts	X	
AxC Address	X	
Miscellaneous	X	
Core Files	X	
Utilities		
Messaging DB Audits (Storage)	X	
Start Messaging	X	X
Stop Messaging	X	
LDAP Status/Restart (Storage)	X	
Change LDAP Password (Storage)	X	
Logs		
Administration History	X	X
Administrator	X	X
Alarm	X	X
Software Management	X	
Maintenance	X	X
IMAP/SMTP Messaging	X	
ELA Delivery Failures	X	
5 of 7		

Table 6: Messaging Web Access Mask default settings

Menu-Item	Fixed (suser)	Editable (user)
	Profile 18	Profile 19
User Activity	X	
System Log Filter	X	
Collect System Log Files	X	
Call Records	X	
Audit/Ports Usage	X	
Diagnostics Results (Application)	X	
Server Reports		
System Evaluation (Storage)	X	
IMAP/SMTP Traffic (Storage)	X	
TCP/IP Snapshot	X	
Measurements (Storage)	X	
Diagnostics		
Alarm Origination	X	
LDAP Test Connection	X	
SMTP Connection	X	
POP3 Connection	X	
IMAP4 Connection	X	
Mail Delivery	X	
Name Server Lookup	X	
Diagnostics (Application)	X	
Telephony Diagnostics (Application)		
Busy	X	
Diagnose	X	
6 of 7		

Table 6: Messaging Web Access Mask default settings

Menu-Item	Fixed (suser)	Editable (user)
	Profile 18	Profile 19
Display	X	
Release	X	
Software Management		
List Messaging Software	X	
Software Install	X	
Software Verification	X	
Software Removal	X	
Advanced Software Install	X	
7 of 7		

Privilege escalation

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

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

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

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

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

Additional information

- [Credentials complexity and expiration requirements](#) on page 58
- [Managing administrative accounts](#) on page 64
- [Administering authentication passwords](#) on page 65

Local host account authentication

Messaging is configured by default to support only local host accounts. A local host account is an account in which all authentication, authorization, and accounting information is maintained on the same server to which the user is attempting access.

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

Chapter 3: Configurable Security

Configurable encryption

- [Avaya's encryption overview](#) on page 35
- [Transport and storage encryption algorithms](#) on page 36
- [Mixing encrypted and nonencrypted policies](#) on page 40
- [Mixing encrypted and nonencrypted policies](#) on page 40

Avaya's encryption overview

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

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

[Table 7: Comparisons in signaling and bearer traffic](#) on page 36 compares how encryption mitigates the vulnerabilities in signaling and bearer media.

Table 7: Comparisons in signaling and bearer traffic

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

Transport and storage encryption algorithms

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

SRTP media encryption for SIP Integration

Messaging supports Secure RTP media encryption based on RFC3711.

Dynamically-generated, symmetric encryption keys are used for encrypting RTP bearer traffic when enabled for SIP-based integration. SRTP for SIP uses RFC 4568 "Session Description Protocol (SDP) Security Descriptions for Media Streams" to distribute the media encryption keys over SIP-TLS signaling channel which is protected with a 128-bit, AES-encrypted TLS connection.

In all of these media encryption solutions, the media encryption keys are dynamically created on a per-connection basis. Separate keys are produced for the "transmit" and "receive" streams of each call. Since all of these keys are dynamically created and assigned, they are stored only in RAM and are not accessible by administrators or users. RTP keys are not escrowed.

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

Table 8: SRTP Encryption supported in Messaging

Encryption Technique	Available algorithms	Description
SRTP		SRTP provides encryption and authentication of RTP streams for calls between SIP-SIP 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

Encryption summary

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

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

[Table 9: Messaging secure protocols](#) on page 38 lists the protocols in Messaging to ensure secure transmissions through data encryption. Keys are dynamically generated and stored in RAM where they are overwritten whenever the link is disabled or recreated.

Table 9: Messaging secure protocols

Link	Description	Transport protocol	Encryption / authentication algorithm	Key exchange
RTP	Bearer traffic (voice calls)	SRTP	AES HMAC-SHA1	Keys are dynamically created on a per-connection basis. Separate keys are produced for the "transmit" and "receive" streams of each call. Keys are not escrowed but are stored in RAM where they are not accessible by administrators or users. In conference calls a unique key pair (one for transmit, one for receive) is assigned for encrypting the payload of each endpoint participating in the conference.
Administrative access	Web interface for server to computer/laptop	HTTPS SSL/TLS	AES 3DES	Keys negotiated each time link is established and are discarded at the end of the session (not retained in flash memory).
1 of 2				

Table 9: Messaging secure protocols

Link	Description	Transport protocol	Encryption / authentication algorithm	Key exchange
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 Messaging software but not accessible by users or administrators exchanged with 128-bit Diffie-Hellman. Since the IPSI link is only between a specific interface card and the media server, the key that is used to secure that link only needs to be known by those two entities.
Account information	Required local account stored on media server; all others on supported external AAA server.			
Backup	Server to data destination: files in the pam_config backup set are included in the security set. For manual movement to another server running the same Messaging release.	SCP	AES-128	15-256 character pass phrase
				2 of 2

Mixing encrypted and nonencrypted policies

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

Authentication files for Messaging

The authentication file contains logins and passwords Avaya Services personnel use to access the Avaya server. Ensure that a valid authentication file exists in the system. If not, the system blocks all access to the Messaging system from any logon.

The authentication file is created on an Avaya services support system and downloaded to the Avaya server. You can only change the file using this support system. To change the authentication information, replace the entire file. If the authentication file is missing or corrupted, the system denies all logins to the Avaya server. This does not prevent the Messaging system from running but blocks further administration until you install a new authentication file through the System Platform console domain.

Note:

If the authentication file is not installed, the system displays an error message that the system cannot display the authentication file information.

About the authentication file

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

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

ASG

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

Starting the AFS application

Prerequisites

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

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

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

Creating an authentication file for a new system

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

1. Start and log in to the AFS application.
2. In the **Product** field, select **SP System Platform**.
3. In the **Release** field, select the release number of the System Platform, and then click **Next**.
4. Select **New System**, and then click **Next**.
5. In the **Communication Manager 6.x** field, enter the fully qualified domain name (FQDN) of the Messaging virtual machine.
6. In the **Utility Server 6.x** field, enter the FQDN of the System Platform Console Domain.

7. If you want to download the authentication file directly from the AFS application to your computer:
 - a. Click **Download file to my PC**.
 - b. Click **Save** in the File Download dialog box.
 - c. Select the location where you want to save the authentication file, and then click **Save**.
 - d. Click **Close** in the Download complete dialog box to complete the download.
After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).
8. If you want to have the authentication file sent in an e-mail message:
 - a. Enter the e-mail address in the **Email Address** field.
 - b. Click **Download file via email**. AFS sends the e-mail message that includes the authentication file as an attachment and the AFID, system type, and release in the message text.
 - c. Save the authentication file to a location on the e-mail recipient's computer.
After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).
9. To view the header information in the authentication file, go to the location where the file is saved and use WordPad to open the file.
The header includes the AFID, product name and release number, and the date and time that the authentication file was generated.

Related topics:

[Starting the AFS application](#) on page 41

Creating an authentication file for a file replacement

Prerequisites

You must have the AFID of the authentication file that you want to replace. See [Obtaining the AFID from System Platform Web console](#) on page 45 or [Obtaining the AFID from Messaging SMI](#) on page 45.

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

1. Log in to the AFS application.
2. In the **Product** field, select **SP System Platform**.
3. In the **Release** field, select the release number of the System Platform, 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 Messaging, read the product access instructions. After reading the instructions, select **I read and understand the Product Access Instructions**.
 - If you do not use an Avaya Services login to access Messaging, select **I do not use Avaya Services logins**.
7. If you want to download the authentication file directly from the AFS application to your computer:
 - a. Click **Download file to my PC**.
 - b. Click **Save** in the File Download dialog box.
 - c. Select the location where you want to save the authentication file, and then click **Save**.
 - d. Click **Close** in the Download complete dialog box to complete the download.
After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).
8. If you want to have the authentication file sent in an e-mail message:
 - a. Enter the e-mail address in the **Email Address** field.
 - b. Click **Download file via email**. AFS sends the e-mail message that includes the authentication file as an attachment and the AFID, system type, and release in the message text.
 - c. Save the authentication file to a location on the e-mail recipient's computer.
After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).
9. To view the header information in the authentication file, go to the location where the file is saved and use WordPad to open the file.
The header includes the AFID, product name and release number, and the date and time that the authentication file was generated.

Related topics:

[Starting the AFS application](#) on page 41

[Obtaining the AFID from System Platform Web console](#) on page 45

[Obtaining the AFID from Messaging SMI](#) on page 45

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

Prerequisites

You must have the AFID of the authentication file on the system that you are upgrading. See [Obtaining the AFID from System Platform Web console](#) on page 45 or [Obtaining the AFID from Messaging SMI](#) on page 45.

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

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

- c. Save the authentication file to a location on the e-mail recipient's computer. After the authentication file is created, AFS displays a confirmation message that contains the system type, release, and authentication file ID (AFID).
9. To view the header information in the authentication file, go to the location where the file is saved and use WordPad to open the file. The header includes the AFID, product name and release number, and the date and time that the authentication file was generated.

Related topics:

[Starting the AFS application](#) on page 41

[Obtaining the AFID from System Platform Web console](#) on page 45

[Obtaining the AFID from Messaging SMI](#) on page 45

Obtaining the AFID from System Platform Web console

1. Start and log in to the System Platform Web Console.
2. In the navigation pane, click **User Administration > Authentication File**. The system displays the AFID in the **AFID** field. The default authentication that is installed with System Platform is an AFID of 7100000000. Replace the default file with a unique file.

Obtaining the AFID from Messaging SMI

1. Start and log in to the Messaging System Management Interface (SMI).
2. Click **Administration > Server (Maintenance)**.
3. In the navigation pane, under **Security**, click **Authentication File**. The system displays the AFID in the **AFID** field. The default authentication that is installed with System Platform is an AFID of 7100000000. Replace the default file with a unique file.

Installing an authentication file

Prerequisites

You must create and download the authentication file from AFS.

System Platform and Messaging share the same authentication file. When you install the authentication file in System Platform, the file is automatically installed on Messaging. To automatically install the authentication file on Messaging, ensure that you have created the user account in Messaging.

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

2. Click User **Administration > Authentication File**.
3. Click **Upload**.
4. In the Choose File to Upload dialog box, find and select the authentication file, and then click **Open**.

Note:

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

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



CAUTION:

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

5. Click **Install**.
The system uploads the selected authentication file and validates the file. The system installs the authentication file if it is valid.
6. To confirm that the authentication file is installed on Messaging, check the Authentication File page of the SMI.

Related topics:

[Obtaining the AFID from Messaging SMI](#) on page 45

Digital certificates and server trust relationships

- [Chain of trust](#) on page 46
- [Avaya Public Key Infrastructure](#) on page 47
- [PKI in Messaging](#) on page 49
- [Managing changes to the Avaya certificate](#) on page 56

Chain of trust

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

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

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

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

The server certificate and the IA certificate are embedded in the authentication file along with the private key associated with the certificate. The Avaya Product Root CA certificate is embedded in the Messaging software base.

Avaya RFA uses a:

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

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

Avaya Public Key Infrastructure

Public Key Infrastructure (PKI) combines software, encryption technologies, and services to enable enterprises to secure their communications and transactions over data networks. A successful PKI provides the management infrastructure to integrate public key technology into your IT infrastructure. Public key technology includes digital certificates, public keys, and certificate authorities.

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

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

Avaya uses standard X.509 PKI to manage certificates in the enterprise in which the hierarchy of certificates is always a top-down tree, with a root certificate at the top, representing the central Certificate Authority (CA) that is integral to the trusted-party scheme and does not need third-party authentication.

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

Messaging uses a consistent PKI model, including the:

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

[Table 10: Key pair and certificate usage](#) on page 48 lists the Avaya public and private keys and their uses.

Table 10: Key pair and certificate usage

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

Note:

The Avaya Product Certificate Authority does *not*:

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

Avaya security certificate types

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 as a trusted CA. If you plan to use this computer and browser to access this or other Avaya servers again, you must install a root certificate after you log in. Your browser authenticates the Avaya server certificate with the root certificate installed in your computer system.

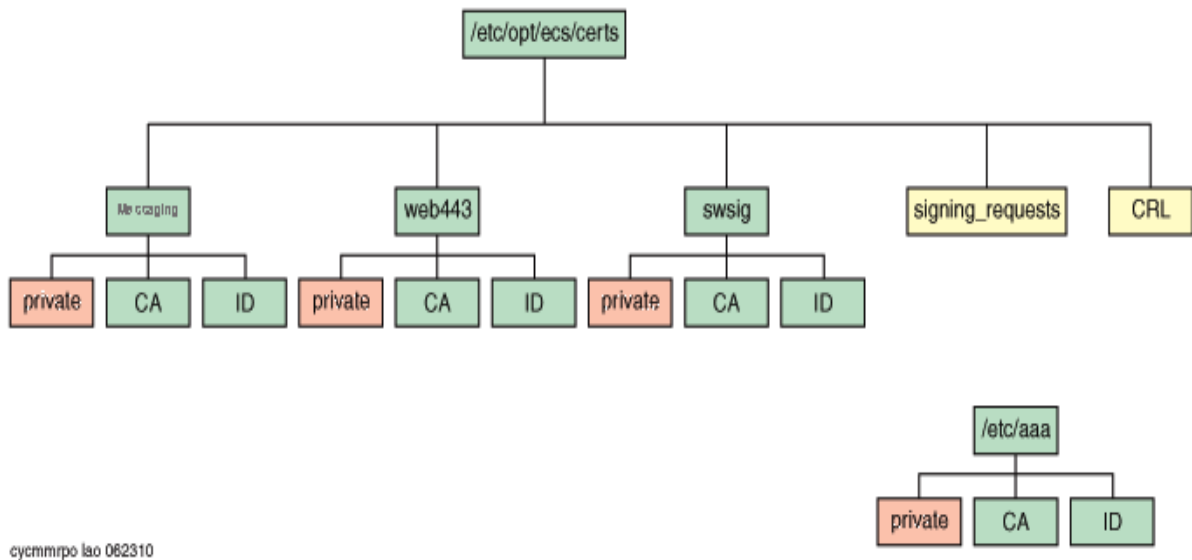
A server certificate verifies the identity of a server. The server certificate changes every time the server is reconfigured. If the server's name is changed the next time you log in, you may get a security alert.

The Avaya server relies on two server certificates. One server certificate is the default certificate used by service technicians (who must log in to many servers to perform tasks). The default certificate is issued to the services Ethernet interface address (192 . 11 . 13 . 6) and identifies the certificate authority as the *SIP Product Certificate Authority*.

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

Avaya certificate repository

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



PKI in Messaging

Messaging conforms to the TLS standard to establish a TLS session. Digital certificates authenticate stages of the TLS session establishment to:

- Establish SIP/TLS connections between IP phones and Messaging through the customer-installed, trusted third-party certificate ([Customers can install their own trusted certificates](#) on page 54).
- Authenticate access to the Messaging Web interface ([Connection to Messaging Web interface](#) on page 56)

- SIP/TLS connections
 - Management
 - Signaling

Install Root Certificate on a PC

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

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



WARNING:

You must install a CA certificate as a Root Certificate.

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

Installing a Root Certificate on a PC

1. Log on to the **System Management Interface**.
2. On the Administration menu, click **Server (Maintenance) > Security > Install Root Certificate**
3. On the **Install Root Certificate** page, click **Install**.
4. In the **File Download - Security Warning** dialog box click **Save**.
5. Select a location and save the *avayaRootCert.cer*.
6. Navigate to the location for *avayaRootCert.cer*, and double-click it.
7. In the **Open File - Security Warning** dialog box, click **Open**.
8. From the **General** tab in the **Certificate** dialog box, click **Install Certificate...**
9. Accept all the default settings in the **Certificate Import Wizard**, and click **Finish**.



Important:

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

Trusted certificates

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



Important:

A trusted certificate must be a Certificate Authority (CA) certificate.

Displaying a trusted certificate on the server

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

Adding a trusted certificate to the server



Important:

A trusted certificate must be a Certificate Authority (CA) certificate.

- From the **Trusted Certificates** page, click **Add**.
- From the **Trusted Certificate - Add** page, enter the file name for the certificate you want to add. The certificate must be in a pem file and located in the `/var/home/ftp/pub` directory.
- To validate the certificate, click **Open**.
After a successful validation, the **Trusted Certificates – Add** page displays the issued-to, issued by, and expiration date information for the certificate you are adding.

Note:

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

- Enter a name for the certificate. Ensure you enter identical names for the certificate you add in each repository.
- Select the repositories to add the certificate, and click **Add**.
The system verifies the following:
 - The certificate name has a `.crt` extension. If the certificate name has a different extension, the system deletes it and replaces it with a `.crt` extension.
 - The certificate name is unique and does not already exist.
 - The certificate is not a duplicate certificate with a new name.

Deleting a trusted certificate from the server

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

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

Removing a trusted certificate on the server from a particular repository

See [Deleting a trusted certificate from the server](#) on page 51.

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

1. From the **Trusted Certificate** page, select a certificate entry, and click **Copy**.
2. From the **Trusted Certificates – Copy** page select the repositories where you want the certificate copied to, and click **Copy**.
The system verifies the following:
 - a. The certificate name is unique and does not already exist.
 - b. The certificate is not a duplicate certificate with a new name.

Note:

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

Server and application certificates

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



Important:

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

The Avaya server provides two server certificates. One certificate is for the service technicians who must log in to many servers. The service technicians' certificate is issued to the services Ethernet interface address (192 . 11 . 13 . 6), and identifies the certificate authority as the Avaya Call Server. The second certificate is issued to the site-specific server name after it is configured.

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

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

Note:

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

Displaying a server or application certificate

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

Adding a server or application certificate to the server

**WARNING:**

You must be a member of the `susers` group to add a server or application certificate.

Prerequisite:

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

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

Note:

To store the certificate the system will not prompt you to enter a file name. The default file name is `server.crt`.

In the case of a single server and application certificate chain, the server sub-directory of a repository is limited to a single file for a single certificate chain. This file is the `server.crt` file. This certificate represents an identity, and only one identity is supported. The system overwrites the existing `server.crt` file, and replaces it with the new one.

Removing a server or application certificate from the server



WARNING:

You must be a member of the `susers` group to add a server or application certificate.

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

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



WARNING:

You must be a member of the `susers` group to add a server or application certificate.

1. From the **Server/Application Certificates** page, select a certificate and click **Copy**.
2. From the **Server/Application Certificates - Copy** page, select the repository to install the selected certificate.
3. Click **Copy**.

Customers can install their own trusted certificates

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

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

- Avaya Product Root Certificate Authority
- SIP Certificate Authority

- Motorola SSECA Root Certificate Authority
- Spectel Root Certificate Authority

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

By using the **tlscertmanage** command (see [Additional information](#) on page 58) at the server command line, customers can load a third-party trusted certificate of their own trusted certificate into the Messaging repository for use the next time Messaging restarts.

Note:

You must restart Messaging before it can recognize and use the newly-installed third-party certificate.

The **all-ca.crt** file can contain up to eight certificates, meaning that the customer may load up to four additional third-party certificates. If more than eight certificates are in the **all-ca.crt** file, Messaging loads the first eight then ignores the remaining certificates and generates a minor alarm (see [Additional information](#) on page 58) and a syslog entry to notify the user that it could not load the file.

Third-party certificate management

[Table 11: Messaging third-party certificate management](#) on page 55 describes how Messaging handles third-party certificates.

Table 11: Messaging third-party certificate management

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

Connection to Messaging Web interface

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

Managing changes to the Avaya certificate

[Table 12: Changes in the Avaya certificate](#) on page 56 lists how Avaya manages changes to its digital certificates.

Table 12: Changes in the Avaya certificate

Type of change	Description
Renewal	Certificates are never renewed. In the event that a certificate expires or is compromised, a new certificate is issued along with a new license file.
Re-key	Certificates are never re-keyed. In the event that a certificate expires or is compromised, a new certificate is issued along with a new license file.
Modification	Certificates are never modified. In the event that certificate content needs to change, a new certificate is issued along with a new license file.
Revocation	Certificates are revoked if the customer, technical support, or members of the Avaya Security Team believes the certificate has been compromised for any reason. Final decision is left to the Avaya Product Certificate Authority. A certificate is revoked in these circumstances: • The information in the certificate is wrong or inaccurate. • The subject has failed to comply with the rules in the policy. • The system to which the certificate has been issued has been retired or is no longer supported.
1 of 2	

Table 12: Changes in the Avaya certificate

Type of change	Description
Who can request revocation?	Certificate revocations can be requested by: • The certificate subscriber • The Registration Authority (RA) that has performed the validation of the certificate request • Any entity presenting proof of responsibility for a certified Avaya SIP product • Any entity presenting proof of the certificate misuse • Any entity presenting proof of the private key compromise The final decision on revocation of the certificate is left to the Avaya Product Certificate Authority.
Procedure for revocation request	The Avaya Product Certificate Authority accepts revocation requests by email only: apca@avaya.com The email must be authenticated and must include the serial number and subject name of the certificate in question.
Revocation request grace period	Avaya determines a timeframe for response at the time of the request.
2 of 2	

Certificate alarms

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

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

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

Creating certificate alarms

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

1. From the **System Management Interface (SMI)** page select **Certificate Alarms**.
2. From the **Certificate Alarms** page select one or all of the following options:
 - Create an warning alarm or a minor alarm between 61 to 180 days before the certificate expires.

- Create an warning alarm, a major alarm, or a minor alarm between 31 - 60 days before the certificate expires.
 - Create a major alarm or a minor alarm between 8 - 30 days before the certificate expires.
3. For each option you selected in option 2, choose the type of warning you want to set from the drop-down box, and the day you want the alarm generated.
 4. Click **Submit**.

Additional information

- Remote Feature Activation (RFA) Web site: <http://rfa.avaya.com>
- Replacing the identify certificate using Simple Certificate Enrollment Protocol (SCEP) in *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Installation and Maintenance Guide*.

Administrative accounts

- [Credentials complexity and expiration requirements](#) on page 58
- [Credentials management](#) on page 61
- [Applying profiles for role-based administration](#) on page 61
- [Managing administrative accounts](#) on page 64
- [Administering authentication passwords](#) on page 65

Credentials complexity and expiration requirements

Messaging logins comply with:

- [Password complexity policies](#) on page 59
- [Credentials expiration and lockout policies](#) on page 59

Password complexity policies

Password complexity rules that apply to passwords for local administrator and user accounts are listed in [Table 13: Password complexity rules for Messaging](#). Attempts to create disallowed passwords result in an instructive error message.

Table 13: Password complexity rules for Messaging

Password complexity rules	Parameters
Minimum length	Default: 6 Allowable values: 3-15
Maximum length	Default: 15 Allowable values: 3-15
The number of days after which the password expires.	Default: 0 Allowable values: 0-999
The number of days before the current password expires and the day the system starts sending the user a warning to change the password.	Default: 0 Allowable values: 0-999
The number of failed login attempts before the system locks the user account.	Default: 0 Allowable values: 0-99
Passwords cannot be in sequential order, ascending or descending.	Messaging enforces the rules.
Password cannot be the same as the extension.	Messaging performs the audit.
Password cannot contain the extension anywhere within the password.	Messaging performs the audit.
Password cannot consist a single repeated digit.	Messaging enforces the rules.

Credentials expiration and lockout policies

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

Note:

This page sets global policy for all logins created through the Server (Maintenance). The following logins must be administered through the root login:

- Logins with credentials located in an external AAA server.

- Logins out of the purview of the global policy.

Note:

Credentials expiration and lockout policies for branch gateways are managed through the gateway's CLI.

Table 14: Login Account Policy fields and parameters

Field	Parameters
Credential Expiration Parameters	
The maximum number of days a password may be used (PASS_MAX_DAYS):	Default: 99999 Allowable values: 1-99999
The minimum number of days allowed between password changes (PASS_MIN_DAYS):	Default: 0 Allowable values: 0-99999
The number of days a warning is given before a password expires (PASS_WARN_AGE):	Default: 7 Allowable values: 0-30
The number of days after a password expires to lock the account (INACTIVE, 0= immediate, 99999=never):	Default: 99999 Allowable values: 0-99999 Note: 0 = immediate 99999 = never
Failed Login Response	
Enable account lock out parameters (PAM Tally)	If not checked, the remaining parameters (below) are ignored.
Lock out account after the following number of unsuccessful attempts (DENY):	Default: 5 Allowable values: 1-9
Automatically unlock a locked account after the following number of seconds (UNLOCK_TIME):	Default: 600 Allowable values: 1-99999
Reset the failed attempt counter after last failed attempt (UNLOCK_RESET):	Default: Yes Allowable values: Yes or No

Password administration recommendations

For Messaging password management, consider the following recommendations and constraints:

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

Credentials management

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

Messaging does not use a database to store credentials information.

- Passwords for local accounts are stored in `/etc/shadow`. Passwords in `/etc/shadow` are stored as a one-way hash. The file `/etc/shadow` is root restricted.
- Usernames and group membership for local Messaging accounts can be viewed by any user logged into Linux.
- ASG accounts have additional information stored in files that are AES encrypted.
- Credentials configured for an external AAA server such as RADIUS or LDAP are stored in the external server.

More information

- [Avaya's encryption overview](#) on page 35

Applying profiles for role-based administration

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

Avaya customers can create and modify profiles to allow access to Avaya server and gateway information according to job functions and business needs. [Table 15: RBAC profile examples](#) on page 62 lists examples.

Table 15: RBAC profile examples

Profile name	Job function and access permissions
Privileged Administrator	The privileged administrator account has the following permissions to access the system: • Read/write access to system parameters, such as IP addresses and software upgrades. • Read/write access to create and modify logins. • Modify, assign, and define user roles. For the procedure on how to create the privileged administrator account, see Creating the privileged administrator account on page 62.
Backup Administrator	Ability to perform only backups and restores.
Security Administrator	Read-write access to create other logins; create, modify or assign roles and profiles; install ASG keys, install licenses, install PKI certificates and keys.
Avaya Maintenance and Support	Access to maintenance logs, run diagnostics.
Auditor	Read-only access to logs and audit files. Read-only permissions prevents unauthorized modification of log files.
Telephony Application Administrator	Read-write access to application configuration, such as trunks
Telephone Provisioning	Ability to add, change, and delete a certain range of telephone extensions
ACD Administrator	Ability to modify call center vectors
Checker	Read-only access, able to only view certain changes

Creating the privileged administrator account

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

1. Log on to the System Management Interface.
2. On the Administration menu, click **Server (Maintenance) > Security > Administrator Accounts**.

3. From the **Select Action**, select **Add Login**.
4. Select **Privileged Administrator**.
5. Click **Submit**.
The system displays the **Administrator Accounts -- Add Login: Privileged Administrator** page.
6. Use [Table 16: Administrator Accounts -- Add Login: Privileged Administrator field descriptions and values](#) on page 63, to fill in the appropriate fields.

Table 16: Administrator Accounts -- Add Login: Privileged Administrator field descriptions and values

Field	Description / Values
Login name	Up to 31 characters (a-z, A-Z, 0-9). The login name cannot already exist or cannot be a protected login name. New or modified ASG customer protected logins requires an AES key.
Primary group	Set to <code>susers</code> and cannot be changed.
Additional groups (profile)	Drop-down menu contains profiles 18 (default) through 69.
Linux shell	Set to <code>/bin/bash</code> and cannot be changed.
Home directory	Updated automatically to <code>/var/home/login-name</code> when the Login name field is populated. The entry cannot be changed.
Lock this account	Select this checkbox if you want to lock the user from logging into the system. (Optional)
Date after which account is disabled blank to ignore (YYYY-MM-DD)	Enter a date when the login should be disabled in the <code>yyyy-mm-dd</code> format or blank (never disabled).
Select type of authentication	● Password ● ASG: enter key (user defined, ASG user information must include the ASG key) ● ASG: Auto-generate key (Messaging automatically generates the ASG key)  WARNING: Selecting this button deactivates the Enter key or password and Re-enter key or password fields.
1 of 2	

Table 16: Administrator Accounts -- Add Login: Privileged Administrator field descriptions and values

Field	Description / Values
Enter password or key	Field can be up to 31 characters, and can include the following: ● lowercase letters of the English alphabet (a-z) ● uppercase or capital letters of the English alphabet (A-Z) ● 0-9 ● periods (.) ● hyphens (-) ● underscores (_) ● dollar sign (\$) ● a blank space ● colons (:) ● semi-colons (;) ● commas (,) ● equal sign (=) ● forward slash (/) ● ampersand (&) ● pound sign (#) ● plus sign (+) ● apostrophe (') ● asterisk (*) ● quotation marks (" ") ● parentheses())
Re-enter password or key	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 next login	Select Yes (requires password change on first use) or No .
2 of 2	

Managing administrative accounts

Avaya provides authentication and access control to the Messaging System Management Interface.

Detailed access control is administered through the interfaces as described in [Table 17: Managing Messaging accounts](#) on page 65.

Table 17: Managing Messaging accounts

Messaging account administration	Interface
Managing Avaya Server web interface login accounts • Adding an administrator account (login) • Changing, locking, removing logins • Adding and removing login groups • Managing passwords	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

Account administration recommendations

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

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

Administering authentication passwords

Passwords for Messaging 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.

Access Security Gateway (ASG)

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

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

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

ASG Guard and ASG Guard Plus

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

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

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

ASG Guard II

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

ASG Guard and ASG Guard II compared

[Table 18: Comparative features: ASG Guard and ASG Guard II](#) on page 67 lists and compares the features of ASG Guard and ASG Guard II.

Table 18: 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

Table 18: Comparative features: ASG Guard and ASG Guard II

Features	ASG Guard	ASG Guard II
Failure history log	Y	Y
Failed authentication alarms	Y	Y
Session buffer	Y	Y
Encrypted connection (IPSec, SSH)	N	Y
Segregate management access from enterprise network	N	Y
Deny/Allow Command	Y	Y
Environmental monitoring (temperature and contact closures)	Y	Y
Phone line consolidation	Y	Y
Collaborative sessions	Y	Y

ASG security products

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

Managing subscriber accounts

Limiting client access

Messaging supports various access mechanisms to mailboxes and messages, greetings, and other configurable features such as Reach Me and MWI. Messaging provides interfaces for certain added functionality, including remote administration and desktop client access to mailboxes. For instance, mailboxes can be accessed via Microsoft Outlook or Zimbra that connects to the customer local area network (LAN). The system can support standard and Secure Sockets Layer (SSL) versions of IMAP4 and SMTP client access on the Storage server. Messaging can also be networked with additional Messaging and voice mail systems.

For customers that wish to block certain access methods for security reasons, the system administrator can block access using one or more of the following techniques:

- Administer privacy settings in the Class of Service (COS).
- Disable access on the Messaging server(s) by disabling the associated ports using the System Management Interface of Messaging.
- Administer an external firewall to restrict access to those ports (i.e. limit to a specific IP address or range).

Telephone user interface (TUI) access

Subscribers traditionally use the telephone user interface (TUI) to access their mailboxes. Messaging uses the mailbox ID and password that the caller provides. Password security requires subscribers to press the pound key (#) after entering their passwords to access their mailboxes. If subscribers do not press the pound key (#), the system pauses before allowing mailbox access. The system can wait for the subscriber to press the pound key (#) or give the subscriber immediate mailbox access after a successful password entry.

Client IP network access

The following clients can access Messaging mailboxes over an IP network:

- Email clients
- Web browser (for User preferences)

The same password policies that apply to TUI access are used for IP-based clients.

E-mail clients via IMAP4

Depending on the system configuration, users can access their mailboxes with mail clients that use the standard IMAP4 protocols.

Depending on the configuration of clients and server, Messaging and the email client can send passwords in encrypted or unencrypted (cleartext) form. Use SSL or Simple Authentication and Security Layer (SASL) to ensure Messaging and clients transport passwords in encrypted form.

SSL versions of the IMAP4, and SMTP protocols are supported by most email clients. For example, users enable SSL encryption while setting up their Messaging account in Outlook or Zimbra. In these configurations, the entire IMAP4 or SMTP conversation is encrypted. Although the Challenge-Response Authentication Mechanism-Message Digest 5 (CRAM-MD5) authentication mechanism can be used (which by itself is not considered strong), transport layer security used by SSL ensures the user password is protected.

For clients connected to Messaging with the Avaya Storage Server, the Storage Server requires SMTP user authentication. The user authentication verifies that the sender of a message is in the domain. This feature ensures that spammers cannot send messages from the system.

Because anyone can observe packets in transit, it's important to use encryption to prevent unauthorized access to subscriber accounts. Customers who want to keep message content private should use only SSL-capable clients. If SSL encryption cannot be used, customers should at a minimum require clients that support CRAM-MD5 authentication.

Messaging supports the SSL protocol for IMAP4 and SMTP. The SSL protocol provides communications privacy over the Internet. The protocol allows applications to communicate in a way that prevents eavesdropping, tampering, or message forgery. Administrators can enable IMAP4 SSL access on the message server. Subscribers can also configure their e-mail clients to use Transport Layer Security (TLS). Subscribers can configure clients for SSL operation over the administered IMAP4 SSL port. The same applies to SMTP.

Web browser (for User preferences)

User preference is a Web-based visual interface that subscribers can use to change default mailbox settings.

For more information about User preference, see the Using Avaya Aura® Messaging guide and the Avaya Aura® Messaging Overview and Planning guide. You can download these documents from the Avaya Support Web site at <https://support.avaya.com/css/Products/P0792>.

Lightweight Directory Access Protocol client access

Messaging provides encrypted Lightweight Directory Access Protocol (LDAP) interfaces that can access directory data. The system can provide full channel encryption through SSL and login and password access through SASL. For more information, see the related topic above, "Trusted Server Administration."

Subscriber mailbox password administration

The administrator enables a subscriber account for voice messaging and determines the initial password for mailbox access. Administrators configure the system to prompt TUI subscribers to change their passwords the first time they access the voice mail system. Administrators can reset a subscriber password at any time but cannot view the password.

The administrator can enable password expiration that forces subscribers to change passwords at predetermined intervals. Changing the password reduces the chance that an unauthorized user can access a subscriber mailbox.

To increase security, administrators can apply the following password (PIN) policies to subscriber mailbox accounts:

- Enforce a minimum password (PIN) length (3 to 15 digits, default is 4). The administrator establishes the minimum password length as a system-wide parameter.
- Enforce password aging, password aging is not enabled by default.
- Force password change the first time a user logs in [To enable, set a nonconforming password, for example a password that is shorter than the minimum password length, and the TUI forces the subscriber to change the password when the subscriber logs in to the mailbox for the first time. The new password must conform to the password setting rules.]
- Block break-in attempts by setting a low lockout threshold (low number of consecutive unsuccessful attempts to log in to a mailbox on the VMSC subscriber page)

The system checks the following parameters to ensure the password is not:

- in sequential order, ascending or descending.
- the same as the extension.
- contain the extension anywhere within the password.
- consist a single repeated digit.

Messaging subscribers gain access to the message server from either a desktop computer or the telephone user interface (TUI). To protect the subscriber mailbox password, ensure the following best practices:

- Use desktop clients that support Secure Sockets Layer (SSL) encryption. Messaging provides native support for SSL versions of IMAP4.
- Never use obvious or unimportant passwords, such as an employee identification number, a social security number, or easily guessed numeric combinations.
- Do not assign a password that is the mailbox number in reverse order, a 1 followed by the mailbox number, or any similar pattern.
- Discourage the practice of writing down passwords, storing them, or sharing them with others. Advise the subscriber to keep any written password in a secure place and to discard an inactive password.
- Never program passwords onto telephone automatic dial buttons.

Set password expiration and complexity features to improve password security.

Toll fraud prevention

- [Limiting long distance access](#) on page 72

Limiting long distance access

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

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

Configuring logging and events

- [Configuring SNMP and syslog](#) on page 73

Configuring SNMP and syslog

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

All syslog files are found under the */var/log* directory, for example the security syslog file */var/log/secure*. The first level subdirectories of */var/log/avaya/messaging* provide log files for the major components of Messaging, for example */var/log/avaya/messaging/mango/messaging.log*.

What security-related events are logged?

Security events are related to the following actions or activities:

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

Note:

You cannot disable logging of security events.

[Table 19: Logging facility and priority for security and non-security events](#) on page 73 shows the syslog priority and facility for security and non-security events.

Table 19: Logging facility and priority for security and non-security events

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

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

- [Configuring SNMP in Messaging](#) on page 74
- [Configuring the syslog server in Messaging](#) on page 75
- [Accessing system logs through the Web](#) on page 77 provides another way to select, filter and view the syslog through the Messaging System Management Interface.
- [Restricting web access to system logs](#) on page 92 has information on how to assign or restrict user access privileges to the syslog.

Configuring SNMP in Messaging

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

Messaging supports the following SNMP versions:

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

Configure SNMP through these Messaging System Management Interface:

- [Agent Status page](#) on page 74
- [SNMP Agents page](#) on page 74
- [SNMP Traps page](#) on page 75

Agent Status page

The order in which you set up SNMP is important. First, disable the SNMP agent at the Messaging System Management Interface (**Alarms > Agent Status** on the left-side navigation pane..

SNMP Agents page

Configure the SNMP agent through the Messaging System Management Interface (**Alarms > SNMP Agents** on the left-side navigation pane.

Note:

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

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

- Block access to the SNMP port

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

SNMP Traps page

The **SNMP Traps** page allows you to specify which alarms are set as traps.

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

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

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

Re-enable SNMP agent

To complete setting up SNMP notifications, go to the [Agent Status page](#) on page 74 and re-enable the SNMP agent.

Messaging security event notifications through SNMP

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

Note:

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

- IPSI downloads and resets
- Messaging platform upgrades (update script)

Configuring the syslog server in Messaging

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

- Avaya maintains a local syslog on the server to facilitate debugging, regardless of whether the customer chooses to log information to an external server.

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

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

Topics in this section include:

- [General syslog guidelines](#) on page 76 details what syslog contains, file synchronization options, and firewall activity for the syslog server.
- [Administering the syslog server in Messaging](#) on page 76 helps you configure the Messaging syslog server.

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. These cannot be disabled through the administrative interface.
- 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 ESS/LSP servers.
- The external syslog server configuration is saved as part of the security backup data set.
- The server firewall automatically opens outbound for the syslog port (514 UDP) if the user enables logging to an external syslog server and automatically closes if logging is not enabled.

Administering the syslog server in Messaging

Note:

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

The Messaging System Management Interface (**Security > Syslog Server** on the left-side navigation pane) displays **Syslog Server** page .

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

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

- Check **Synchronize syslog configuration to all LSP and ESS servers** if you want to synchronize the main server's syslog configuration to any administered LSP/ESS server(s).
- The **Select Which Logs Are to be Sent to the Above Server** section allows you to select the logs that you want to send to the external syslog server:
 - Security log (var/log/secure)
 - Command history log (var/log/ecs/command history)
 - Messaging IP events log (/var/log/messages)
 - kernel, boot, cron, *.info, *.emerg logs (/var/log/messages)

Accessing system logs through the Web

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

This form allows you to:

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

More information

- [Restricting web access to system logs](#) on page 92
- [Reading and interpreting the security logs](#) on page 93

Chapter 4: Network Security Integration

Network "best practices"

- [Separation of network functionality](#) on page 79
- [Layer 2 and Layer 3 hardening](#) on page 80
- [Designing VLAN groups for functional network segmentation](#) on page 80
- [How ARP spoofing facilitates network attacks](#) on page 81
- [Security strategies to combat ARP spoofing](#) on page 82
- [Security vulnerabilities with name and address management](#) on page 82
- [How Messaging addresses NIST recommendations](#) on page 83
- [How Messaging addresses the vulnerability: On Messaging systems, Telnet is disabled by default. SSH is the recommended protocol for remote access. In addition, physical access through a serial console is available on every Messaging server.](#) on page 86

Separation of network functionality

Control and bearer signaling in VLANs

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

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

Note:

Separation of the LAN may not be possible for some customers.

Layer 2 and Layer 3 hardening

To ensure the Messaging system is secure, it is recommended that the customer harden, or secure, devices in the communication system's network at Layer 2, the data link layer, and Layer 3, the network layer, as defined by the Open Systems Interconnect (OSI) 7-layer network model. Messaging offers logging capabilities (see [Configuring SNMP and syslog](#) on page 73), which the customer can use to detect actual and potential security breaches. Additional host intrusion and network intrusion detection systems can also be added to the customer's network to detect security breaches at Layers 2 and 3.

The customer can also use a number of security features in other devices in the network to harden Layers 2 and 3 of the network. These devices include the G250-series, G350 Media Gateways, G430/G450 Media gateways, the IG550 Integrated Gateway, and third-party Ethernet switches and routers that provide LAN/WAN connectivity.

Note:

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

Designing VLAN groups for functional network segmentation

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

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

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

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

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

Traffic filtering and firewalling between VLANs

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

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

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

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

How ARP spoofing facilitates network attacks

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

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

Security strategies to combat ARP spoofing

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

Avaya recommends the following practical defenses:

- Dividing the network into separate domains or subnets.

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

Security vulnerabilities with name and address management

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

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

DNS vulnerabilities

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

DNS security

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

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

How Messaging addresses NIST recommendations

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

- [Confidentiality and privacy](#)
- [Integrity issues](#)
- [Availability and Denial of Service](#)

Confidentiality and privacy

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

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

- [Switch default password vulnerability](#) on page 84
- [Classical wiretap vulnerability](#) on page 84
- [ARP cache poisoning and ARP floods](#) on page 85
- [Web server interfaces](#) on page 85
- [IP phone subnet mask vulnerability](#) on page 97
- [Extension to IP address mapping vulnerability](#) on page 97

Switch default password vulnerability

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

How Messaging addresses the vulnerability: Messaging enforces default password change at the time of Messaging server installation. A super-user login must be administered before the installation can be completed.

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

Classical wiretap vulnerability

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

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

How Messaging addresses the vulnerability: Messaging logs events such as the disconnect of an IP telephone are reported to Messaging. In addition, an alarm is generated when an IP telephone is disconnected. See *Maintenance Commands for Avaya Servers, and Media Gateways*, 03-300430

ARP cache poisoning and ARP floods

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

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

How Messaging addresses the vulnerability: See [Security strategies to combat ARP spoofing](#) on page 82.

Web server interfaces

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

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

How Messaging addresses the vulnerability: By default Messaging uses HTTPS over SSL and TLS.

Integrity issues

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

- An intruder masquerades as a legitimate user and accesses an operations port of the system. Then, the intruder can perform such operations as:
 - Disclosing confidential data
 - Causing service deterioration by modifying the system software
 - Crashing the system
 - Removing all traces of the intrusion (for example, modifying the security log)
- At certain times the system becomes vulnerable because it is not in a secure state. For example:
 - After a system restart or during a disaster recovery, the old security features may have been reset to insecure settings, and new features might not yet be activated. (For example, all old passwords might have reverted to the default system-password, even though new passwords are not yet assigned.)

- At the time of installation the system may be vulnerable until the default security features have been replaced.

Availability and Denial of Service

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

Default password vulnerability

See [Switch default password vulnerability](#) on page 84.

Account lockout vulnerability

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

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

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

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

Chapter 5: Operational Security

Avaya Security Advisories

- [What is an Avaya Security Advisory](#) on page 87
- [How do I get Avaya Security Advisories?](#) on page 88
- [How to interpret an Avaya Security Advisory](#) on page 89

What is an Avaya Security Advisory

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

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

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

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

When a security vulnerability is identified, the PSST determines susceptibility of Avaya products to those vulnerabilities and assigns one of four risk levels: **High**, **Medium**, **Low**, and **None** (see [How to interpret an Avaya Security Advisory](#) on page 89). Depending on the category of risk, the PSST creates an Avaya Security Advisory to notify customers of the vulnerability.

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

How do I get Avaya Security Advisories?

Avaya Security Advisories are posted on the Security Support Web site at <http://support.avaya.com/security>. The PSST also sends email to customers who have signed up to receive advisories. The advisories are distributed in a time frame as indicated in [Table 20: Avaya Security Advisories time frames](#) on page 88:

Table 20: 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's discretion

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

1. Browse to <http://support.avaya.com>.
2. Select **My E-notifications** on the right side of the page
3. If you do not have an account click on **Registration Now** and follow the instructions.
4. Log in using your existing credentials.
5. Select **Add New E-notifications**.
6. Click **Submit**.
7. Select **Security Advisories** and click **Continue** to receive notifications on creation or update of all security advisories.
To receive notification on creation or update of security advisories of a specific product select a product from the product list and skip to step 9.
8. Select **Security Advisories** and click **Submit** to ensure that **E-notifications** is added. Skip to step 11.
9. From the release version page select the product version and click **Continue**.
10. Select **Security Advisories** in **Avaya Support E-Notifications Service** page and click **Submit**.

11. A confirmation page appears.

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

How to interpret an Avaya Security Advisory

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

[Table 21: Avaya's security vulnerability classification](#) on page 89 summarizes the three main categories.

Table 21: Avaya's security vulnerability classification

Vulnerability classification	Criteria for classification
High	The product is vulnerable to: • Attacks from a remote unauthenticated user who: – Can easily access high-level administrative control of a system or critical application without interaction with a user of the product beyond standard operating procedures. • Attacks from remote unauthenticated user who: – Can easily cause the system or a critical application to shutdown, reboot, or become unusable without requiring interaction with a product user. For example, see the advisory at http://support.avaya.com/elmodocs2/security/ASA-2006-002.htm.
Medium	The product does not meet criteria for high vulnerability, but is vulnerable to: • Attack from a user who can access a user account, and access does not directly require the privileges of a high-level administrative account. • The system and/or critical application shutting down, rebooting, or becoming unusable, and an existing administrative or local account is used for this attack. • Attack from a user who can access a local user account from which higher-level privileges are available. For example, see the advisory at http://support.avaya.com/elmodocs2/security/ASA-2006-262.htm
1 of 2	

Table 21: Avaya's security vulnerability classification

Vulnerability classification	Criteria for classification
Low	The product does not meet criteria for medium or high vulnerability, but is vulnerable to: ● Compromise of the confidentiality, integrity, or availability of resources, although any compromise is difficult or unlikely without non-standard direct user interaction. ● Non-critical applications shutting down, rebooting, or becoming unusable. For example, see the advisory at http://support.avaya.com/elmodocs2/security/ASA-2007-015.htm.
None	A related third-party product has a vulnerability but the affected software package(s), module(s), or configuration(s) are not used on an Avaya product and there is therefore no vulnerability. For example, see the advisory at http://support.avaya.com/elmodocs2/security/ASA-2006-261.htm.
2 of 2	

How an advisory is organized

Each Avaya Security Advisory contains the following information:

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

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

- A description of the risk
- Instructions on how to correct the problem, which might include:
 - Installing an update
 - Revising administration of the product
- A description of what additional security fixes, if any, are included in the update.
- **Avaya Software-Only Products** — A listing of the specific Avaya products that use, but are not bundled with, operating system software that might be vulnerable. Information includes:
 - The product version affected
 - Possible actions to take to reduce or eliminate the risk

- **Avaya System Products** — A listing of the specific Avaya products that are vulnerable or are bundled with operating system software that might be vulnerable. Information includes:
 - The level of risk
 - The product version affected
 - Possible actions to take to reduce or eliminate the risk
- **Recommended Actions** — A list and description of steps to take to remove the vulnerability. The steps might include installing a security update, administering a security feature, or performing a software upgrade. For operating system and third-party software, the recommended actions are normally identified in detail through the Web site links in the security advisory.

How Avaya incorporates security updates in its applications

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

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

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

Logging, monitoring and audit trails

- [Removing old accounts](#) on page 92
- [Restricting web access to system logs](#) on page 92
- [Where is security information logged?](#) on page 92
- [Reading and interpreting the security logs](#) on page 93

Removing old accounts

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

Remove administrator accounts on the **Security > Administrator Accounts** page as described in *Administering Avaya Aura™ Messaging*.

Restricting web access to system logs

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

For more information see:

- [System Management Interface default profiles and permissions](#) on page 24 for the default permission setting for Profile 18 (superuser) and Profile 19 (user).
- A complete discussion of the **Web Access Mask** page is in *Administering Avaya Aura™ Messaging*.

Where is security information logged?

Security information is logged in or notified through:

- SNMP trap receiver (see [Configuring SNMP and syslog](#) on page 73)
- Syslog security log (see [Configuring the syslog server in Messaging](#) on page 75)
- Miscellaneous logs that track security-related information:
 - Linux access security log
 - Platform command history log
 - HTTP/web access log
 - IP events
 - Platform bash command history log

Reading and interpreting the security logs

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

Topics in this section include:

- [Interpreting the syslog header](#) on page 93
- [Interpreting SNMP entries in the syslog](#) on page 94
- [Interpreting the platform command history log](#) on page 95
- [Software and firmware updates](#) on page 96
- [Interpreting the command history log for Web activity](#) on page 119

Interpreting the syslog header

Each syslog entry has a common header format:

yyyymmdd:hh:mm:sssss text

Table 22: Syslog entry header format description

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

Syslog header example

20070326:061058000:7103:cmds:MED:

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

Syslog server example for a branch gateway

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

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

Figure 1: Syslog server for G430 gateway

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

Interpreting SNMP entries in the syslog

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

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

Table 23: SNMP agent log description

Log entry	Description
module-name	The name of the SNMP module logging the event
pid	The Linux process ID of the process initiating the log entry
snmp	The text string "snmp"
ip	The ip address of the management system
1 of 2	

Log entry	Description
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.
2 of 2	

SNMP log example

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

Note:

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

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

Interpreting the platform command history log

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

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

Table 24: 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
1 of 2	

Field	Description
server-name	The host name of this server
text	The text field contains the log event text that is supplied by the module logging the event. For more information on the text field see the following section: • Interpreting the command history log for Web activity on page 119
2 of 2	

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 almcalls
```

```
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**, **almcalls**, **almenable**, and **serialnumber**.

Software and firmware updates

- [How Avaya delivers security updates](#) on page 96
- [Applying an operating system security update](#) on page 98
- [Applying an Avaya field load or software update](#) on page 99

How Avaya delivers security updates

Generally, Avaya makes security updates available on or through the Avaya Security Web site at <http://support.avaya.com/security>. In addition, Avaya incorporates security updates, if applicable, in subsequent software release packages.

Based on the classification of vulnerability and the availability of a vendor-supplied update, Avaya makes a best effort attempt to provide remediation actions based on the following target intervals:

Table 25: Vulnerability classifications and remediation intervals

Vulnerability	Target remediation intervals
High	If Avaya needs to develop a software update, the Avaya Security Advisory provides a timeline for availability of the update. Avaya incorporates the fix into a separate service pack or update (30 days maximum delivery time). If a software patch is available for installation or another action is recommended, the Avaya Security Advisory describes the actions.
Medium	If Avaya needs to develop a software update, Avaya includes the update in the next major release that can reasonably incorporate the update. If no new major releases are scheduled for a product, and Avaya is providing maintenance support, Avaya incorporates the fix into a separate service pack or update (1 year maximum delivery time). If a software patch is available for installation or another action is recommended, the Avaya Security Advisory describes the actions.
Low	If Avaya needs to develop a software update, Avaya includes the update in the next major release that can reasonably incorporate the update. If no new major releases are scheduled for a product, and Avaya is providing maintenance support, Avaya incorporates the fix into a separate service pack or update (1 year maximum delivery time). If a software patch is available for installation or another action is recommended, the Avaya Security Advisory describes the actions.
None	No remediation actions are required.

Avaya product development staff incorporates a third-party update into its software in one of three ways:

- Avaya simply bundles the specific update or the new release of the affected software with the Messaging software such that the security-related updates are automatically incorporated into the Avaya product operation.
- Avaya modifies the Messaging software so that the specific update or the new release of the affected software is appropriately incorporated into the Messaging 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 Messaging operation.

When Avaya incorporates one or more security fixes into its software, the fixes might be delivered in one of three forms:

- A security update
A security update includes operating system and/or third-party software security fixes.
- An Avaya software update
An Avaya software update includes software security fixes to the Avaya application software.
- An Avaya full release of software
An Avaya full release of software includes all software for the Avaya product, including software security fixes to the Avaya application software and/or security fixes for the operating system and third-party fixes.

Validating a security update

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

Avaya-generated security updates are likewise tested on all affected products prior to release. Avaya security updates are likewise tested before incorporation into subsequent releases.

Testing meets requirements of internal Avaya testing standards, including testing for the following:

- Denial of Service
- Encryption standards
- Certificate management
- Audits and logging
- Access control

Applying an operating system security update

Operating system security updates for Messaging servers are typically applied separately from other platform or Messaging software updates. If Avaya issues a security update, the customer might apply the update themselves or engage their service support group to apply it.

Instructions for applying a security update are normally provided either in the security advisory or as instructions on the Web site for updates of the associated operating system or application package. See <http://support.avaya.com/security>.

- For Messaging, see the Administering Avaya Aura® Messaging guide.

- For System Platform, see the Administering Avaya Aura® System Platform guide.

Applying an Avaya field load or software update

An Avaya field load, or software update, is an update of the Avaya product software. In some cases, a security-related change to Avaya software may result in the creation of a Messaging software update.

If Avaya issues an Avaya software update, the customer might apply the update themselves or engage their service support group to apply it. In most cases, the customer is responsible for applying the update unless the customer's Maintenance contract includes automatic software updates. In some cases, only services personnel have permission to apply the update.

Software updates are posted on the Avaya Download Center. An Avaya customer must register with the Download Center to obtain a login, and then the customer can access the Avaya update software applicable to the customer's products. Instructions for applying a security update are normally provided either in the security advisory or as instructions on the Download Software Web site.

For Messaging, the System Management Interface facilitates applying a software update. In such cases, product documentation, as well as the associated security advisory, describes how to use the interface to install the update. See "Installing security and Messaging service pack updates" in *Installing and Upgrading the Avaya S8300 Server (555-234-100)*.

Determining the contents of a security update

For each security update for a third-party application or the Linux operating system, the referencing security advisory provides a link for quick access to the third-party Web site. Such Web sites typically provide a description of the security fixes that are included in the update.

For a security update for Messaging, the referencing security advisory provides a link to an Avaya Web page or FTP site that stores the update and a readme file that describes the security fixes in the update.

Avaya may package multiple third-party security updates together for installation on Messaging. Such packages are cumulative and include all security updates previously available and applicable to the product. In many cases, once the package is installed, the customer can use Messaging's Manage Software Web page to locate the update file name.

The customer can then determine the contents with the following steps:

1. Access the Avaya support Web page at <http://support.avaya.com>.
2. Select Download Software.
3. Select Messaging.
4. Select **Latest TN Circuit Pack, Media Server, and Media Gateway Firmware and Software Updates**.

5. Select the appropriate G.A. load of Messaging software.
6. Select the **Latest S8x00 Media Server Service Pack Update Contents**.
7. Select **Contents of Latest Service Pack for S8500**.
8. View the readme file for the security update package.

In Messaging Release 4 or higher, the customer can run the Linux command **update_info <security patch name>**, where **<security patch name>** is the name of the Avaya security update. The resulting display identifies each Avaya security advisory number. The customer can then access the Avaya Security Web page and view the contents for each security advisory.

Regulatory issues

- [Considerations for customers who must comply with the Sarbanes-Oxley Act](#) on page 100
- [Considerations for customers who must comply with the Graham-Leach-Bliley Act](#) on page 103
- [Considerations for customers who must comply with HIPAA](#) on page 104
- [Considerations for customers who must comply with CALEA](#) on page 105
- [Considerations for customers who must comply with FISMA](#) on page 106
- [Considerations for customers who want to comply with ISO 17799](#) on page 107
- [Considerations for customers who must comply with E911](#) on page 110
- [Considerations for non-US customers who must comply with regulations](#) on page 111

Considerations for customers who must comply with the Sarbanes-Oxley Act

Note:

This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the act's requirements. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The Sarbanes-Oxley Act of 2002 is a federal law enacted in response to a number of accounting scandals involving major U.S. corporations. A key requirement of the act is that public companies evaluate and disclose the effectiveness of their internal controls as they relate to financial reporting. One major area of internal control consists of information technology controls. As a result, the Sarbanes-Oxley Act holds chief information officers responsible for the security, accuracy and the reliability of the systems that manage and report the financial data.

To the extent that a company uses data collected or transmitted by Messaging as part of its overall cost or revenue reporting and financial management, the company can use security-related features of Messaging to secure the data. Use of these features can further demonstrate the company's good faith data management and reporting.

Messaging security features also help prevent unauthorized access to the customer's network, in general.

See [Table 26: Data security features in this guide](#) on page 101 for features related to data security and documented in more detail in other sections of this document.

Table 26: Data security features in this guide

Feature	How related to Sarbanes-Oxley	Where documented
Encryption	Transmitted data is protected from packet-sniffing and eavesdropping	See: • Avaya's encryption overview on page 35
Access control	Access to data is protected from unauthorized personnel	See: • Access profiles on page 24 • Managing administrative accounts on page 64
Authentication	Access to the system is restricted by login/password.	See: • Access profiles on page 24 • Managing administrative accounts on page 64
Logging	Security-related events are logged	See: • Configuring SNMP and syslog on page 73 • Reading and interpreting the security logs on page 93
Backup of data	Data saved on backup media or backup server. Protected by encryption and key.	See: • Secure backups of Messaging data and translations on page 113

Messaging data used for financial purposes

Messaging can generate call detail records that might be used in financial data:

- Messaging generates call detail records in real-time and sends the records to a device the customer specifies. The device can be a printer or a reporting system that converts call record data into financial records. Two such reporting systems, eCAS Call Accounting System and VeraSmart Application Suite, are available through Avaya DeveloperConnect partner Veramark Technologies, Inc. These devices provide their own data security. For more information, see <http://www.veramark.com/products/verasmart.htm>.
- Messaging transmits Call Detail Recording (CDR) records to call accounting devices over a TCP/IP connection using Avaya's proprietary Reliable Session Protocol. While the data are protected from corruption, the data are not encrypted. For this reason, where possible, the customer should cable the CDR device directly to the Messaging server, whenever possible, for the export of CDR data.
- The customer may add the following financial data elements for inclusion in CDR records:
 - Account codes are codes that users can manually enter identify the purpose or the associated client of each call. Messaging includes account codes in CDR records when account codes are enabled.
 - Advice of Charge (AOC, for ISDN trunks) is charge information that Messaging collects from the public network for each outgoing call. Charge advice is a number representing the cost of a call; it might be recorded as either a charging or currency unit.
 - Periodic Pulse Metering (PPM, for non-ISDN trunks) is data that Messaging based on the pulses transmitted from the public network at periodic intervals during an outgoing trunk call. At the end of the call, the number of pulses collected is the basis for determining charges.

Other adjunct systems collecting Messaging data

The Avaya Call Management System (CMS) and the Avaya Interactive Response system both collect call data that might be used to generate financial reports. Like the CDR reporting devices, these systems have a number of security features that can be used to protect data.

The CMS communicates with Messaging over a TCP/IP connection using a proprietary binary protocol. The Interactive Response system communicates with Messaging using a TCP/IP connection. The customer can enhance the Interactive Response connection by using TLS and SRTP protocols.

For more information on Interactive Response security, see http://support.avaya.com/elmodocs2/ir/r2_0/print_Security.pdf.

For more information on Call Management System security, see "Avaya Call Management System Security Whitepaper."

Considerations for customers who must comply with the Graham-Leach-Bliley Act

Note:

This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the act's requirements. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The Gramm-Leach-Bliley Act (GLB) requires financial institutions to disclose privacy policies regarding customer data. This disclosure must describe the ways the institution may use and disclose private information.

Where indicated in their policy, financial institutions must protect the privacy of their customers, including customers' nonpublic, personal information. To ensure this protection, the Graham-Leach-Bliley Act mandates that all institutions establish appropriate administrative, technical and physical safeguards.

Messaging data to which the Graham-Leach-Bliley Act might apply includes customer names and telephone numbers, called and calling number data, and abbreviated dial lists.

Use of the following key features can protect customer privacy and demonstrate the company's compliance with the interagency guidelines supporting the Graham-Leach-Bliley Act.

Table 27: Messaging security and compliance of Graham-Leach-Bliley Act

Feature	How related to Graham-Leach Bliley Act	Where documented
Encryption	Transmitted and stored data is protected from unauthorized individuals.	See: • Avaya's encryption overview on page 35
System access control	Access to data is protected from unauthorized personnel.	See: • Access profiles on page 24 • Managing administrative accounts on page 64
Authentication	Access to the system is restricted by login/password.	• Access profiles on page 24 • Managing administrative accounts on page 64
Backup of data	Protection against destruction, loss, or damage of customer information due to potential environmental hazards or technological failures; protected by encryption and key	See • Secure backups of Messaging data and translations on page 113

Considerations for customers who must comply with HIPAA

Note:

This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the act's requirements. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires health care providers to disclose to health care recipients the ways in which the institution may use and disclose private information. HIPAA also requires health care providers to protect the privacy of certain individually identifiable health data for health care recipients.

Messaging data to which HIPAA might apply includes customer names and telephone numbers, and called and calling number data.

Use of the following key features can protect patient privacy and demonstrate the health care provider's compliance with HIPAA.

Table 28: Messaging security and compliance of HIPAA

Feature	How related to HIPAA	Where documented
Encryption	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate	See: • Avaya's encryption overview on page 35
System access control	Implement technical policies and procedures for electronic information systems that maintain electronically-protected health information to allow access only to those persons or software programs that have been granted access rights.	See: • Managing administrative accounts on page 64

1 of 2

Feature	How related to HIPAA	Where documented
Authentication	Implement procedures to verify that a person or entity seeking access to electronically-protected health information is the one claimed.	See: • Access profiles on page 24 • Managing administrative accounts on page 64
Backup of data	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronically-protected health information.	See: • Managing administrative accounts on page 64
2 of 2		

Considerations for customers who must comply with CALEA

Note:

This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the act's requirements. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

In response to concerns that emerging technologies such as digital and wireless communications are increasing the difficulty for law enforcement agencies to execute authorized surveillance, Congress enacted the Communication Assistance for Law Enforcement Act (CALEA) in 1994. CALEA is intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that the systems support the necessary surveillance capabilities of law enforcement agencies.

In an order effective September 23, 2005, the FCC concluded that CALEA applies to facilities-based broadband Internet access providers and interconnected VoIP service providers. To the extent that CALEA applies to Avaya offerings, such offerings have achieved compliance with the applicable CALEA requirements. In the event that an Avaya customer is subject to CALEA requirements, there are various third-party products, including Session Border Controller products, that claim to provide or facilitate CALEA compliance.

Examples of these products are:

- NexTone
- AcmePacket
- Sipera

In addition, Messaging characteristics that can aid in CALEA compliance are the following:

- Messaging use of standard architectures. For example:
 - Messaging uses Open Systems Interconnection (OSI) standards for network communications. Therefore, transmissions are interceptable for surveillance tools established to work with the OSI standards.
 - Messaging telephone calls are always divided into call control signaling and voice or bearer signaling. This simplifies the task of determining what data to surveil.
- Messaging assurance of the authenticity and integrity of the calls being surveilled through its encryption and authentication capabilities.
- Call Detail Records, which records called numbers, and other call data that might be useful to law enforcement.

Finally, Messaging offers the service observing feature, which allows monitoring of calls with or without awareness of the parties on the call.

Considerations for customers who must comply with FISMA

Note:

This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the act's requirements. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The Federal Information Security Management Act of 2002 provides for development and maintenance of minimum controls required to protect Federal information and information systems. Telecommunications systems and commercially-developed information security systems are included in the systems referenced under this act.

As a result, in most cases, government agencies can use security-related features of Messaging to secure telecommunications data. Messaging security features can also help prevent unauthorized access to the customer's network, in general.

Features related to system security and documented in more detail in other sections of this document are listed in [Table 29: Messaging security and compliance of FISMA](#) on page 107.

Table 29: Messaging security and compliance of FISMA

Feature	How related to FISMA	Where documented
Encryption	Transmitted data is protected from packet-sniffing and eavesdropping and other unauthorized access.	See: • Avaya's encryption overview on page 35
System access control	Access to data is protected from unauthorized personnel	See: • Managing administrative accounts on page 64
Authentication	Access to the system is restricted by login/password.	See: • Administering authentication passwords on page 65
Logging	Security-related events are logged	See: • Configuring SNMP and syslog on page 73 • Reading and interpreting the security logs on page 93
Firewall	Access to Messaging network is protected	See: • Firewall protection on page 18
Backup of data	Data saved on backup media or backup server. Protected by encryption and key	See • Secure backups of Messaging data and translations on page 113
Toll fraud prevention	Unauthorized use of long-distance is prevented	See • Limiting long distance access on page 72

Considerations for customers who want to comply with ISO 17799

ISO 17799 of the International Standards Organization, "Information technology - Security techniques - Code of practice for information security management," is an internationally-accepted standard of good practice for information security. ISO 17799 suggests a well structured set of controls to address information security risks, covering confidentiality, integrity and availability aspects. None of the suggested controls is mandatory, however, an organization wishing to be in compliance should show a security strategy that explains the decision not to implement key controls.

See [Table 30: Messaging security and compliance of ISO 17799](#) on page 108 on how ISO 17799 addresses the different categories of data security management.

Table 30: Messaging security and compliance of ISO 17799

ISO 17799 Security Guidelines	Messaging features and processes
Ensure that applications process information correctly	
● Use validation checks to control processing	Use the System Log and Maintenance Alarm and Event logs. See: ● Configuring SNMP and syslog on page 73 ● Reading and interpreting the security logs on page 93
● Validate data input into your applications	Messaging can track administration and notify the administrator when changes are made. Use the System Log, and the Maintenance Alarm and Event logs. See: ● Configuring SNMP and syslog on page 73 ● Reading and interpreting the security logs on page 93
● 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 46 ● Administering authentication passwords on page 65
● Validate your applications' output data	Use audits and status reports to verify output.
● Use cryptographic controls to protect your information	Encrypt data to protect data from packet-sniffing and eavesdropping. See: ● Avaya's encryption overview on page 35 ● Secure updates of Avaya software and firmware on page 113
1 of 3	

ISO 17799 Security Guidelines**Messaging features and processes****Protect and control your organization's system files**

Control the installation of operational software	Messaging requires the appropriate access control in order to install software. In addition, a digital certificate from the software ensures the software is allowed to be installed on the server. See Security problems addressed by digital certificates on page 23 Secure updates of Avaya software and firmware on page 113
Control the use of system data for testing	Avaya uses internal ISO-certified testing processes for software.
Control access to program source code	Messaging source code is not accessible outside of Avaya. The Red Hat Linux operating system is also restricted. See Benefits of Linux operating system for Messaging on page 17

Control development and support processes

Establish formal change control procedures	Avaya uses internal ISO-certified change control processes for software. For security-related updates, Avaya uses a change policy as documented in How Avaya delivers security updates on page 96.
Review applications after operating system changes	Avaya uses internal ISO-certified test procedures after operating system changes. See Validating a security update on page 98.
Restrict changes to software packages	Avaya includes only the Linux software packages it needs for Messaging. Messaging 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	Messaging does not have antivirus, antiworm, or antitrojan software. However, Avaya does not recommend using third-party antivirus software on Messaging. For more information, see Planning against viruses and worms and other malicious code on page 20.

ISO 17799 Security Guidelines	Messaging features and processes
Control outsourced software development	Avaya software, if outsourced, is developed according to Avaya's ISO-certified processes.
Control your technical system vulnerabilities	Messaging offers many features and processes to protect the customer's communications network. See: Avaya's encryption overview on page 35 Managing administrative accounts on page 64 Configuring SNMP and syslog on page 73 Chain of trust on page 46 Avaya Public Key Infrastructure on page 47 Configuring SNMP and syslog on page 73 Secure backups of Messaging data and translations on page 113 Secure updates of Avaya software and firmware on page 113
3 of 3	

Considerations for customers who must comply with E911

Note:

This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the act's requirements. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

In 2005 the U.S. Federal Communications Commission issued the order, IP-Enabled Services and E911 Requirements for IP-Enabled Service Providers, First Report and Order and Notice of Proposed Rulemaking. The order required providers of interconnected voice over Internet Protocol (VoIP) service to supply enhanced 911 (E911) capabilities to their customers. However, these acts currently apply only to telephone and IP telephony service providers and *not* to enterprise telephony users. Therefore, the E911 Act does *not* currently apply to Messaging.

However, the Occupational Safety and Health Administration (OSHA) might consider failure to implement E-911 as a direct violation of Section 5(a)(1) of the Occupational Safety and Health Act, also known as the General Duty Clause, which requires employers to furnish a workplace which is free from recognized hazards, which may cause, or are likely to cause, death or serious physical harm.

In addition, there are roughly 17 states with current or pending legislation requiring enterprise switches to be able to dial 911 and report the caller's number, associated with a physical location. The customer must check with the regulations of the customer's state to clarify what state requirements might exist regarding 911 calling for enterprises providing telephone systems for employees.

Messaging compliance with 911

Traditional telephony

Messaging supports both 911 and E911 requirements. For traditional telephones calling the 911 emergency number, Messaging uses its automatic routing table to send the emergency call over an ISDN trunk and include the Calling Party Number for automatic identification by the PSAP. In this way, the PSAP, using its Automatic Location Information (ALI) database, can immediately identify the location of the emergency. Alternatively, Messaging can send the call to the Public Safety Answering Point (PSAP) through a Centralized Automatic Message Accounting (CAMA) trunk, which sends Caller Emergency Service Identification (CESID) to the PSAP.

For communications systems supporting geographically dispersed locations for which there are different PSAPs, Messaging supports a separate CAMA, ISDN, or central office trunk for each location so that the 911 call and location identification is sent to the correct PSAP.

IP telephony

For IP telephones, SIP-enabled telephones, or Softphone, all of which do not have a physical connection to the Messaging server or gateways but access the communications system over the LAN, Messaging uses the subnetwork to identify the location of the telephone. Messaging then converts this location into an Emergency Location Information Number (ELIN) and passes the ELIN on to the PSAP. For Softphone only, Messaging also allows the user to enter a phone number which the PSAP can then use to identify the user's location during an emergency call. For some types of E911 locating capabilities, the Cielo E-911 Manager from RedSky Technologies, Inc. offers more precise location capabilities. Contact RedSky for more information about how that product interacts with Messaging E911 capabilities. The Web site for RedSky Technologies, Inc. is <http://www.redskytech.com>.

Considerations for non-US customers who must comply with regulations

Any specific country might have unique regulations that raise compliance issues for Messaging. 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, Messaging, through its authentication processes, access control, and encryption methods, can protect call detail records, as well as

the calls to customers. In this way, Messaging can help a customer comply with banking secrecy laws and protect the integrity of its business. Messaging also offers these security features to protect administered data that might reveal a customer's identity, as might be the case, for example, if a customer's IP address or phone number is contained within the firewall rules established for Messaging.

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, Messaging 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 Messaging is sold, there might be a need to inform customers about Messaging 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 Messaging might help the customer comply with regulations.

Common Criteria

The Common Criteria for Information Technology Security Evaluation (CC) and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Agreement (CCRA), which ensures that:

- Products' security properties are evaluated by competent and independent licensed laboratories to determine their assurance.
- Supporting documents that are used within the Common Criteria certification process define how the criteria and evaluation methods are applied when certifying specific technologies.
- The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation.
- These certificates are recognized by all the signatories of the CCRA.

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 Messaging data and translations](#) on page 113
- [Secure updates of Avaya software and firmware](#) on page 113

Secure backups of Messaging data and translations

With Messaging, the customer can use some or all of the following methods to keep data secure during backups:

- The use of the Secure Copy Protocol (SCP) to back up and restore data over a LAN connection.
- The use of role-based accounts to authenticate permissions to backup data.
- The use of password-protected accounts over the LAN for the backup of data.

Note:

The customer must remember the password used for backups in order to restore the data. The password is not retrievable from Messaging.

- The use of a 15- to 256-character pass phrase for encryption of the backup of data.

Note:

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

Secure updates of Avaya software and firmware

The ability to install software or firmware on Messaging 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.

In addition, upgrade firmware and software for some Avaya products, such as the G250, G350, G430 and G450 Media Gateway, the IG550 Integrated Gateway, and TN circuit packs, is signed according to RSA encryption guidelines. Messaging authenticates the software or firmware signature upon attempts at installation. If the authentication or certificate does not match, the installation either fails or, in some cases, a warning appears with an option to continue the installation. See Firmware Download Procedures at <ftp://ftp.avaya.com/incoming/Up1cku9/tsoweb/firmware/TNpackFirmwareDownloadInstructions.pdf>.

When an Avaya server serves as a software or firmware repository from which the software or firmware is downloaded to other Avaya devices, the server provides a certificate for authentication by the downloading device. For example, Messaging server provides HTTPS file service for IP telephones. When IP telephones attempt to download firmware from a Messaging server over a TLS session, the server provides a certificate for authentication. See *Downloading Avaya 46xx IP Telephone Software Using Avaya Media Servers* at http://support.avaya.com/elmodocs2/white_papers/TFTP_HTTP_Download_External_060504.pdf.

For Messaging, the transfer of files between a repository and Messaging server or between Messaging and other Avaya devices can be accomplished using the Secure Copy protocol (SCP). 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 SystemsSM access products at customer sites. for security audits (for example, perimeter scans, penetration tests) and to update and service equipment firmware and alarms, respectively. Using either IP connectivity or traditional dial-in (modem) access, SAC offers service at two levels:

- **SAC Basic** collects alarms from Avaya Products, including modem based alarms, and sends them to Avaya over a B2B VPN/Frame Relay link. Inbound access to products is controlled by SSDP and the customer's firewall.
- **SAC Premium** builds on SAC Basic by adding inbound gateway functionality to the SSG. The customer uses the SSG to control and monitor Avaya's access to their network and products and to record what product was accessed, by whom, when, and why the product was accessed.

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

SSDP firewall and wireless access

Avaya uses a firewall/VPN product called Secure Gateway 2000 (formerly a VPNNet product) on the B2B link. This IPsec, 3DES VPN firewall interoperates with other VPN firewall vendors' products like Cisco, Nortel, and NetScreen.

The DMZ is firewalled off from the rest of the Avaya network. Additional firewalls and intrusion detection systems are deployed throughout the Avaya network partitioning customer servers from other Avaya users.

Remote laptops and desktops use a VPN client to gain wireless access to the Avaya network. They first must connect to the WEP-protected WLAN, then authenticate on the VPN network, and then on the Avaya LAN network.

Remote technicians first access the Avaya LAN using VPN clients. They then authenticate using SSDP's Single Sign-On technology. Authentication and data streams are all encrypted over the WAN.

Remote password complexity and expiration parameters

Avaya programs system that require secure access to meet its password security policy which dictates the password length and complexity as well as the period of time during which a password cannot be reused. Password length, uniqueness, and repetition restriction are in line with industry practices and are implemented in each of the platforms and applications. The system sends warning to users whose password is about to expire.

Appendix A: Physical interfaces and associated network services

Messaging is available on the following servers.

Table 31: Avaya servers

Server	Reference document
Dell™ PowerEdge™ R610	Installing the Dell™ PowerEdge™ R610 Server
HP DL360 G7	Installing the HP DL360 G7 Server
Avaya S8800	Maintaining the Avaya S8800 1U Server for Avaya Aura® Messaging
Avaya S8730	Maintaining the S8730 server for Modular Messaging

Appendix B: Internet ports and protocols

Your IT infrastructure needs to allow network traffic to move freely to and from the Messaging system. The following table lists services used by Messaging, and associated protocol and port number.

For the System Platform ports, see Administering Avaya Aura® System Platform on the Avaya Support Web site at <http://support.avaya.com/css/Products/P0585>.

Some considerations for using the following tables:

- Directions:
 - Inbound: The port is open for external access to the server.
 - Outbound: The server transmits data externally over the port.
- Configure: The port value can be changed by the customer from the SMI.
- Enable/Disable: The port can be enabled and disabled by the customer from the SMI.
- Server Type: Application server, Storage server, or both.
- X: The service or option is available.

Table 32: LAN ports used by Messaging servers

Service Name	Protocol	Port	Direction	Configure	Enable/Disable	Server Type	Notes
ftp	TCP	21	Inbound Outbound		X	Both	
ssh	TCP	22	Inbound Outbound		X	Both	
telnet	TCP	23	Inbound Outbound		X	Both	
smtp	TCP	25	Inbound Outbound	X	X	Both	
dns	UDP	53	Outbound			Both	
http	TCP	80	Inbound			Both	Redirects to HTTPS by default

Table 32: LAN ports used by Messaging servers

Service Name	Protocol	Port	Direction	Configure	Enable/Disable	Server Type	Notes
pop3	TCP	110	Inbound	X	X	Both	
ntp	TCP	123	Outbound			Both	
imap	TCP	143	Inbound	X	X	Both	
snmp	UDP	161	Inbound Outbound			Both	
snmptrap	UDP	162	Inbound Outbound			Both	
ldap	TCP	389	Inbound	X		Both	
http	TCP	443	Inbound			Both	
smtps	TCP	465	Inbound Outbound	X	X	Both	
syslog	TCP	514	Inbound			Both	
ldaps	TCP	636	Inbound Outbound	X	X	Both	
imaps	TCP	993	Inbound	X	X	Both	
pop3s	TCP	995	Inbound	X	X	Both	
hp-sshd	TCP	2222	Inbound		X	Both	
h248-binary	TCP	2945	Inbound			Both	
secure-sat	TCP	5022	Inbound		X	Both	Avaya proprietary use (unused) - secure System Access Terminal
sat	TCP	5023	Inbound		X	Both	Avaya proprietary use (unused) - System Access Terminal
sip	TCP	5060	Inbound Outbound	X		Application	
sip tls	TCP	5061	Inbound Outbound	X		Application	

Table 32: LAN ports used by Messaging servers

Service Name	Protocol	Port	Direction	Configure	Enable/Disable	Server Type	Notes
speechify TTS	TCP	5555	Inbound			Both	Avaya proprietary use - Used to translate text to speech
java-aic	TCP	7117	Inbound			Both	Avaya proprietary use - AxC
java-mwil listener	TCP	7121	Inbound			Both	Avaya proprietary use - MWI Listener
java-aicweb	TCP	7171	Inbound			Both	Avaya proprietary use - AxC web server
adcs-jax	TCP	8081	Inbound Outbound			Both	Avaya proprietary use
adcs-fetch	TCP	8083	Inbound Outbound			Both	Avaya proprietary use - cluster communications
N/A	UDP	1024-65534	Outbound			Application	Used by several protocols to reach clients, including RTP/SRTP
mcapi	TCP	55000	Inbound Outbound	X		Both	Avaya proprietary use - legacy mail access API
N/A	ICMP		Inbound Outbound			Both	Used for "ping" support

Table 33: LAN ports used by Messaging adjuncts

Service Name	Protocol	Port	Direction	Message Networking	one-X Speech	one-X Mobile	one-X Portal
ftp	TCP	21	Inbound Outbound				
ssh	TCP	22	Inbound Outbound				

Appendix B: Internet ports and protocols

Service Name	Protocol	Port	Direction	Message Networking	one-X Speech	one-X Mobile	one-X Portal
telnet	TCP	23	Inbound Outbound				
smtp	TCP	25	Inbound Outbound	X	X	X	X
dns	UDP	53	Outbound				
http	TCP	80	Inbound				
pop3	TCP	110	Inbound				
ntp	TCP	123	Outbound				
imap	TCP	143	Inbound		X	X	X
snmp	UDP	161	Inbound Outbound				
snmptrap	UDP	162	Inbound Outbound				
ldap	TCP	389	Inbound	X	X	X	X
http	TCP	443	Inbound				
smtps	TCP	465	Inbound Outbound	X		X	X
syslog	UDP	514	Inbound				
ldaps	TCP	636	Inbound Outbound	X			X
imaps	TCP	993	Inbound			X	X
pop3s	TCP	995	Inbound				
hp-sshd	TCP	2222	Inbound				
h248-binary	TCP	2945	Inbound				
secure-sat	TCP	5022	Inbound				
sat	TCP	5023	Inbound				
sip	TCP	5060	Inbound Outbound				

Service Name	Protocol	Port	Direction	Message Networking	one-X Speech	one-X Mobile	one-X Portal
sip tls	TCP	5061	Inbound Outbound				
speechify TTS	TCP	5555	Inbound				
java-aic	TCP	7117	Inbound				
java-mwilistener	TCP	7121	Inbound				
java-aicweb	TCP	7171	Inbound				
adcs-jax	TCP	8081	Inbound Outbound				
adcs-fetch	TCP	8023	Inbound Outbound				
N/A	UDP	1024-6 5534	Outbound				
mcapi	TCP	55000	Inbound Outbound				
N/A	ICMP		Inbound Outbound				

Appendix C: Additional security resources

Security documents on the Avaya Support site

Security-related documents that complement this security guide are listed in [Table 34: Security related documents](#) on page 125.

Table 34: Security related documents

Document title	Link
Avaya's Security Vulnerability Classification	http://support.avaya.com/css/P8/documents/100066674
Avaya's Toll Fraud & Security Handbook	http://support.avaya.com/css/P8/documents/100073832

Index

Numerical

3rd-party antivirus products [21](#)

A

access control lists
 configuring packet filtering routers or Layer 3 switches [81](#)
Access Security Gateway (ASG) [19](#), [65](#)
 ASG Guard [68](#)
 credentials storage [61](#)
 description. [66](#)
 product line [68](#)
Address Resolution Protocol (ARP). [82](#)
 spoofing
 Domain Name System (DNS) [82](#)
 Dynamic Host Configuration Control (DHCP) . . . [82](#)
 spoofing tool [82](#)
Apache Web server [23](#)
Avaya Installation Wizard
 Web Access Mask default settings [26](#)
Avaya Product Security Support Team (PSST) [87](#)
 Avaya Security Advisory
 interpretation [89](#)
Avaya Security Advisory [91](#)
 organization [90](#)
 response times based on vulnerability [88](#), [97](#)
 vulnerability levels [87](#)

C

certificates
 location and permissions [56](#)
 modifications [56](#)
 rekeyed [56](#)
 renewal [56](#)
 revocation [56](#)
Communication Manager
 local host account (default) [33](#)

D

Denial of Service (DoS) attacks
 Chargen packet storm [23](#)
 Finger of death. [23](#)
 Fraggle [22](#)
 malformed or oversized packets. [23](#)

Index

Packet relay attack	22
PING flood.	22
Smurf/Pong	22
SNMP PROTOs	23
SPANK	23
SYN flood (TCP SYN)	22
Domain Name Server (DNS)	
remedies	83
enable DNSSEC encryption and support	83
separate DNS servers.	83
Domain Name System (DNS)	
vulnerabilities	82
Dynamic Host Configuration Control (DHCP)	
vulnerabilities	82

E

encryption	
algorithms	
3DES	61
SRTP	37
ASG accounts	61
certificate authority	47
Avaya Product Certificate Authority	56 , 57
digital certificates.	46
mixing encryption policies.	40
public-key integration.	48
Avaya Product PKI	48
external authentication	
credentials storage.	61

F

file system sharing protocols (unsupported)	
Common Internet File System (CIFS)	21
Network File System (NFS)	21
Server Message Block (SMB).	21
FTP	19

G

G250 Media Gateway	
leveraging security features for Layer 2 and Layer 3 hardening	80

H

hard drive partitioning	18
HTTPS connection	
to Apache Web server	23

I

IG550 Integrated Gateway	80
ingress network services.	18

IPSec	20
-----------------	--------------------

L

Linux operating system	
hardening	18
logging/monitoring	
privilege escalation.	32
superuser	32

M

Maintenance Web Pages	
access to Communication Manager	24
Agent Status page	74
default profiles	24
IPTables firewall	18
Profile 18 permissions	25
Profile 19 permissions	26
SNMP Agents page	74
SNMP Traps page	75
Syslog Server page	76
System Logs page	77
Web Access Mask default settings	25

N

National Institute of Standards and Technology (NIST)	
remedies	
availability and denial of service	86
account lockout vulnerability	86
confidentiality and privacy	83
ARP cache poisoning/floods	85
default password	84
packet sniffer/protocol analyzer	84
Web server interfaces	85
integrity issues	85
security risks in VoIP systems.	83
network separation	
802.1X authentication	80
restricting VLAN traffic	81
standard network services	80
stateful filtering.	81
VLAN design	80
non-secure protocols	
FTP	19
TELNET.	19

O

Open Systems Interconnect (OSI)	80
operating system	
Linux	
hardening	17 , 18

Red Hat Package Management (RPM) [17](#)

P

passwords
 where stored. [61](#)
privilege escalation
 logging location [32](#)
Product Security Support Team (PSST) [87](#)

R

Red Hat Package Management (RPM)
 modules removed [17](#)
regulatory compliance
 FISMA [106](#)
regulatory compliance (non-USA) [111](#)
 Basel II [112](#)
regulatory compliance (USA)
 CALEA [105](#)
 E/911 [110](#)
 IP telephony [111](#)
 traditional telephony. [111](#)
 Gramm-Leach-Bliley Act [103](#)
 HIPAA. [104](#)
 ISO 17799. [107](#)
 Sarbanes-Oxley Act [101](#)
role based access control (RBAC)
 privilege escalation. [32](#)
 role evaluation [62](#)
 SAT and Web profile administration [61](#)

S

S8800
 Overview [117](#)
secure protocols
 DES. [75](#)
 MD5. [75](#)
 Secure Copy (SCP) [20](#), [113](#)
 Secure Shell (SSH) [18](#), [20](#)
 SNMPv3. [20](#), [74](#), [75](#)
Secure Socket Layer (SSL) [18](#)
security notifications
 SNMP and syslog [73](#), [80](#)
 syslog [75](#)
 administration [76](#)
 logging levels [77](#)
 priority and facility. [73](#)
 where logged [92](#)
security updates
 contents [99](#)
 field load or software update [99](#), [113](#)
 operating system. [98](#)

vulnerability levels and remediation intervals	96
Simple Authentication and Security Layer (SASL) .	61 , 65
SIP-TLS connections	
PKI integration (digital signatures).	23
SNMP	
community strings	20
SNMPv3	20 , 74 , 75
SNMPv3/v2c	
community name.	20
software update	
3rd-party	91
superuser	
see user account/profile	32
syslog	
log interpretation	93
header	93
platform command history log	95
SNMP entries.	94
restricting Web access to	92
stored locally or exported to external server	75

T

TELNET	19
toll fraud	72
Transport Layer Security (TLS).	20 , 48
Tripwire.	80

U

user account/profile	
credentials storage	61
default Maintenance Web Page accounts	24
password aging	59
password complexity	59
privilege escalation.	19 , 32
removing old accounts	92
role based access control (RBAC).	24 , 25
service accounts	
password aging.	65
superuser	
logging location	32
permissions and restrictions	32

V

viruses	
effects on VOIP system.	20

W

worms	
effects on VOIP system.	20

